Managing Host and Cluster Lifecycle

Update 3

VMware vSphere 8.0
VMware ESXi 8.0

vmware by Broadcom

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://docs.vmware.com/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Managing Host and Cluster Lifecycle

Managing Host and Cluster Lifecycle provides information about configuring and using VMware® vSphere Lifecycle Manager to manage the ESXi hosts and clusters in your environment.

Managing Host and Cluster Lifecycle provides instructions for configuring vSphere Lifecycle Manager, working with the vSphere Lifecycle Manager depot, and using baselines and images to install, update, or upgrade the software and firmware running on your ESXi hosts.

Managing Host and Cluster Lifecycle also provides detailed guidelines about using vSphere Lifecycle Manager recommended images and performing hardware compatibility checks on single hosts or clusters. It also describes how you can configure and use the Update Manager Download Service (UMDS) to download software updates in deployments with no access to the Internet.

At VMware, we value inclusion. To foster this principle within our customer, partner, and internal community, we create content using inclusive language.

Intended Audience

This information is intended for experienced system administrators who are familiar with data center operations and virtual machine technology.

Client Interface

The instructions in this guide reflect the HTML5-based vSphere Client.

Updated Information

This *Managing Host and Cluster Lifecycle* document is updated with each release of the product or when necessary.

This table provides the update history of the *Managing Host and Cluster Lifecycle*.

Revision	Description
26 JUNE 2024	■ Updated the list of supported Linux-based operating systems for installing the Update Manager Download Service (UMDS). See Supported Linux-Based Operating Systems for Installing UMDS.

What is vSphere Lifecycle Manager

1

VMware vSphere® vSphere Lifecycle Manager enables centralized and simplified lifecycle management for VMware ESXi hosts through the use of images and baselines.

Lifecycle Management in vSphere

Lifecycle management refers to the process of installing software, maintaining it through updates and upgrades, and decommissioning it.

In the context of maintaining a vSphere environment, your clusters and hosts in particular, lifecycle management refers to tasks such as installing ESXi and firmware on new hosts, and updating or upgrading the ESXi version and firmware when required.

vSphere Lifecycle Manager Overview

vSphere Lifecycle Manager is a service that runs in vCenter Server and uses the embedded vCenter Server PostgreSQL database. No additional installation is required to start using that feature. Upon deploying the vCenter Server appliance, the vSphere Lifecycle Manager user interface becomes automatically enabled in the HTML5-based vSphere Client.

vSphere Lifecycle Manager encompasses the functionality that Update Manager provides in earlier vSphere releases and enhances it by adding new features and options for ESXi lifecycle management at a cluster level.

In vSphere releases earlier than 7.0, Update Manager provides you with the ability to use baselines and baseline groups for host patching and host upgrade operations. Starting with vSphere 7.0, vSphere Lifecycle Manager introduces the option of using vSphere Lifecycle Manager images as an alternative way to manage the lifecycle of the hosts and clusters in your environment. You can also use vSphere Lifecycle Manager to upgrade the virtual machine hardware and VMware Tools versions of the virtual machines in your environment.

vSphere Lifecycle Manager can work in an environment that has access to the Internet, directly or through a proxy server. It can also work in a secured network without access to the Internet. In such cases, you use the Update Manager Download Service (UMDS) to download updates to the vSphere Lifecycle Manager depot, or you import them manually.

vSphere Lifecycle Manager Operations

The basic vSphere Lifecycle Manager operations are related to maintaining an environment that is up-to-date and ensuring smooth and successful updates and upgrades of the ESXi hosts.

Operation	Description
Compliance Check	An operation of scanning ESXi hosts to determine their level of compliance with a baseline attached to the cluster or with the image that the cluster uses. The compliance check does not alter the object.
Remediation Pre-Check	An operation that you perform before remediation to ensure that the health of a cluster is good and that no issues occur during the remediation process.
Remediation	An operation of applying software updates to the ESXi hosts in a cluster. During remediation, you install software on the hosts. Remediation makes a non-compliant host compliant with the baselines attached to the cluster or with the image for cluster.
Staging	An operation that reduces the time ESXi hosts spend in maintenance mode. When you stage an image or baseline to an ESXi host, vSphere Lifecycle Manager downloads the respective bulletins or components from the vSphere Lifecycle Manager depot to the host without applying them immediately. Staging makes the components, patches, and extensions available locally on the hosts. You can choose to remediate the hosts at a later time, not immediately after staging.

The vSphere Lifecycle Manager Depot

Several components make up vSphere Lifecycle Manager and work together to deliver the vSphere Lifecycle Manager functionality and coordinate the major lifecycle management operations that it provides for. The vSphere Lifecycle Manager depot is an important component in the vSphere Lifecycle Manager architecture, because it contains all software updates that you use to create vSphere Lifecycle Manager baselines and images. You can use vSphere Lifecycle Manager only if the vSphere Lifecycle Manager depot is populated with components, add-ons, base images, and legacy bulletins and patches.

For more information about software updates and how they are distributed, see Software Packaging Units That vSphere Lifecycle Manager Can Consume.

For more information about the vSphere Lifecycle Manager depot, see Chapter 2 The vSphere Lifecycle Manager Depot.

Secure Hashing and Signature Verification in vSphere Lifecycle Manager

vCenter Server performs an automatic hash check on all software that vSphere Lifecycle Manager downloads from online depots or from a UMDS-created depot. Similarly, vCenter Server performs an automatic checksum check on all software that you manually import into the vSphere Lifecycle Manager depot. The hash check verifies the sha-256 checksum of the downloaded software to ensure its integrity. During remediation, before vSphere Lifecycle Manager installs any software on a host, the ESXi host checks the signature of the installable units to verify that they are not corrupted or altered during the download.

When you import an ISO image into the vSphere Lifecycle Manager depot, vCenter Server performs an MD5 hash check on the ISO image to validate its MD5 checksum. During remediation, before the ISO image is installed, the ESXi host verifies the signature inside the image.

If an ESXi host is configured with UEFI Secure Boot, the ESXi host performs full signature verification of each package that is installed on the host every time the host boots. For more information, see the *vSphere Security* documentation.

vSphere Lifecycle Manager Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

Read the following topics next:

- The vSphere Lifecycle Manager User Interface in the vSphere Client
- Using vSphere Lifecycle Manager with VMware vSphere® Distributed Services Engine™
- Software Packaging Units That vSphere Lifecycle Manager Can Consume
- vSphere Lifecycle Manager Baselines and Images
- What Are the Requirements for Using vSphere Lifecycle Manager
- Required Privileges for Using vSphere Lifecycle Manager and vSphere Configuration Profiles

The vSphere Lifecycle Manager User Interface in the vSphere Client

After you deploy the vCenter Server appliance, vSphere Lifecycle Manager becomes immediately visible in the vSphere Client.

The vSphere Lifecycle Manager user interface has two main views, which for convenience this guide calls the home view and the compliance view.

vSphere Lifecycle Manager Home View

The vSphere Lifecycle Manager home view is where you configure and administer the vSphere Lifecycle Manager instance that runs on your vCenter Server system. You go to the vSphere Lifecycle Manager home view to configure how vSphere Lifecycle Manager baselines and images work.

You do not need any special privilege to access the vSphere Lifecycle Manager home view.

To access the vSphere Lifecycle Manager home view in the vSphere Client, select **Menu > Lifecycle Manager**.

In the vSphere Lifecycle Manager home view, you specify the vSphere Lifecycle Manager instance that you want to administer by selecting a vCenter Server system from the drop-down menu at the top of the **Lifecycle Manager** pane.

In the **Lifecycle Manager** pane, you have the following top-level tabs: **Image Depot**, **Updates**, **Imported ISOs**, **Baselines**, and **Settings**.

You use the **Image Depot** tab when you work vSphere Lifecycle Manager images. You use the **Updates**, **Imported ISOs**, and **Baselines** tabs when you work with vSphere Lifecycle Manager baselines. For more information about the **Image Depot**, **Updates**, and **Imported ISOs** tabs, see Browsing the vSphere Lifecycle Manager Depot.

The **Settings** tab is where you configure all vSphere Lifecycle Manager remediation settings and download sources. You use the **Settings** tab with both vSphere Lifecycle Manager images and baselines. For more information about how to configure the vSphere Lifecycle Manager settings, see Chapter 3 vSphere Lifecycle Manager Remediation Settings.

In the vSphere Lifecycle Manager home view, you can perform the following tasks:

- Browse the vSphere Lifecycle Manager depot.
- Trigger the synchronization of updates with the configured online depots.
- Trigger the synchronization of hardware compatibility data.
- Import offline depots manually.
- Import ISO images to use for the creation of upgrade baselines.
- Create and manage baselines and baseline groups.
- Configure the default vSphere Lifecycle Manager download source.
- Add a URL to an online depot to the list of download sources.
- Allow or disallow downloading from a download source.
- Configure host remediation settings.
- Configure virtual machine rollback settings.

vSphere Lifecycle Manager Compliance View

The vSphere Lifecycle Manager compliance view is where you perform the major vSphere Lifecycle Manager operations - checking the compliance of ESXi hosts against a baseline or an image, staging, remediation pre-checks, remediation, and so on.

You go to the vSphere Lifecycle Manager compliance view to actually use the vSphere Lifecycle Manager baselines and images on your clusters and hosts.

To access the vSphere Lifecycle Manager compliance view in the vSphere Client, you must have the **View Compliance Status** privilege.

Generally, the vSphere Lifecycle Manager compliance view is on the **Updates** tab for a selected object.

Depending on the selected object and whether you use baselines or images to manage the object, you access the vSphere Lifecycle Manager compliance view in two different ways.

- To access the vSphere Lifecycle Manager compliance view for a host or a cluster that you manage with baselines, go to the **Updates** tab for the object and select **Baselines**.

  In the **Baselines** pane of the vSphere Lifecycle Manager compliance view, you can perform the following tasks:

  - Check the compliance status of ESXi hosts and clusters against baselines or baseline groups.
  - Attach and detach baselines and baseline groups to hosts and clusters.
  - Generate a remediation pre-check report that lists recommended actions to ensure successful remediation.
  - Stage patches or extensions to hosts.
  - Check the compliance status of ESXi hosts against an image.
  - Remediate hosts against baselines and baseline groups.
  - Remediate hosts that are part of a vSAN cluster against system-managed baselines.
- To access the vSphere Lifecycle Manager compliance view for a cluster or a standalone host that you manage with a single image, go to the **Updates** tab for the object and select **Image**.

  In the **Image** pane of the vSphere Lifecycle Manager compliance view, you can perform the following tasks:

  - Export, import, and edit the image that the cluster or the standalone host use.
  - Upgrade the firmware of the ESXi hosts in the cluster or the standalone host.
  - Check for and view recommended images for the cluster or the standalone host.
  - Check the hardware compatibility for a selected ESXi version against vSAN HCL.
  - Check the compliance status of the ESXi hosts in the cluster or the standalone host against the image.

- Run a remediation pre-check to ensure successful remediation.
- Remediate the ESXi hosts against the image that the cluster or the standalone host use.

On the **Updates** tab, you can also perform other tasks.

- Under **Hosts**, select **Hardware Compatibility** to check the hardware compatibility of a host against the VMware Compatibility Guide.
- Under **Hosts**, select **VMware Tools** or **VM Hardware** to check the status of virtual machines and upgrade the VMware Tools version or the virtual hardware version of the virtual machines.

vSphere Lifecycle Manager and vCenter Server Single Sign-On Domain

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can configure the settings for each vSphere Lifecycle Manager instance. The modifications to the settings are applied only to the vSphere Lifecycle Manager instance that you specify and are not propagated to the other instances in the group. Similarly, you can use vSphere Lifecycle Manager to perform compliance and status checks, and remediate only those inventory objects that are managed by the vCenter Server system where the respective vSphere Lifecycle Manager instance runs.

Using vSphere Lifecycle Manager with VMware vSphere® Distributed Services Engine™

vSphere Distributed Services Engine provides you with the ability to offload some of the network operations from your server CPU to a data processing unit, or the so-called DPU device on the server. You can use vSphere Lifecycle Manager images and all vSphere Lifecycle Manager operations to manage the life cycle of the software and firmware that runs on the DPU devices of your servers.

Using DPU devices for network acceleration frees up the CPU capacity for business-critical workloads. Besides accelerating networking performance, using DPU devices provides security and compression acceleration.

What Is a DPU Device?

A DPU device is a high-performance network interface card, with added embedded CPU cores, memory, and a hypervisor running on the device independently from the ESXi hypervisor installed on the server. DPU devices are like limited-resource servers with multiple general-purpose compute cores.

The ESXi hypervisor that runs on the DPU device is a fully functional hypervisor, but it can only run on ARM CPU architectures. You don't use ESXi on the DPU to run and provision virtual machines and workloads. The hypervisor that runs on DPU devices is a trimmed version of the ESXi hypervisor that runs on your servers. This trimmed ESXi version is optimized for I/O activities, such as packet offloads, external management, and so on.

From vSphere perspective, the DPU device is a pre-configured device that you can start using without any further configuration or customizations.

You cannot manage DPU devices separately from managing your ESXi hosts. All lifecycle operations that you use to manage the lifecycle of the software and firmware on your hosts are used to also manage the software and firmware lifecycle of DPU devices in a DPU-based environment.

The only DPU devices that vSphere 8.0 supports are NVIDIA BlueFeild and Pensando Distributed Services Card (Pensando DSC).

How Do I Start Using a Server with a DPU Device?

To be able to use the advantages that vSphere Distributed Services Engine offers, your server must include a supported DPU device. You cannot purchase a DPU device separately and insert it into a legacy non-DPU server.

To start utilizing the DPU device on a server to offload network services, you must perform a fresh ESXi install on the server. You can perform the installation through interactive or scripted mechanisms. During installation, ESXi is installed both on the server and on the DPU device. In vSphere 8.0, the ESXi image contains VIBs for both the ESXi version to be installed on a host and the ESXi version to be installed on the DPU device on that host.

Managing the Lifecycle of the ESXi and Firmware on a DPU Device

You use vSphere Lifecycle Manager to upgrade the ESXi version and firmware on a DPU device. The VIBs that are needed to upgrade the DPU device are included in the base ESXi images that VMware distributes and that you have in the vSphere Lifecycle Manager depot. You don't need to take care of the software and firmware on a DPU device separately. For example, during remediation vSphere Lifecycle Manager updates ESXi both on the host and on the DPU device. In vSphere 8.0 Update 3, vSphere Lifecycle Manager operations happen in parallel on both DPU devices for hosts with dual DPU setup.

Almost all vSphere Lifecycle Manager operations work for DPU-based environments. In vSphere 8.0, only the following vSphere Lifecycle Manager operations don't work for clusters with DPU-backed hosts:

- Recommendation generation
- Hardware compatibility checks

Solutions Interoperability with vSphere Distributed Services Engine

NSX is the only solution that is allowed to push VIBs to ESXi on the server, on the DPU, or both. Currently, no other solutions can work together with the vSphere Distributed Services Engine.

System Requirements for Using vSphere Distributed Services Engine

- ESXi 8.0 or later
- vCenter Server 8.0 or later

Limitations to Using vSphere Lifecycle Manager for a DPU-Backed Cluster

- The vSphere Distributed Services Engine works for clusters and standalone hosts that you manage with a single vSphere Lifecycle Manager image. You cannot add a host with a DPU device to a cluster that you manage with baselines.
- A host can have one or two DPU devices. If a host has two DPU devices, they must run the same firmware and hardware revisions.
- Each host in the DPU-based cluster must have a DPU device.
- All hosts must have DPU devices from the same vendor and of the same model. The DPU generation might vary.

Software Packaging Units That vSphere Lifecycle Manager Can Consume

VMware and other software vendors create and package their software updates into specific units that vSphere Lifecycle Manager can consume. The smallest packaging construct is the component. Components can be further grouped into larger software units, such as add-ons and base images.

vSphere Lifecycle Manager uses software from VMware, original equipment manufacturers (OEMs), and third-party software providers.

- OEMs are VMware partners, for example, Dell, HPE, VMware Cloud on AWS.
- Third-party software providers are providers of I/O filters, device drivers, CIM modules, and so on.

What Is a vSphere Installation Bundle (VIB)?

The VIB is the basic building block for the creation of installation packages for ESXi hosts. A VIB is a software package that contains metadata and a binary payload, which represents the actual piece of software to be installed on an ESXi host. The VIB does not represent an entire feature, but just a single module of the feature. So, the VIB is the smallest installable software unit that VMware and other software vendors ship.

Starting with vSphere 8.0, a VIB can install software on either the ESXi running on the host or the ESXi running on a DPU device on the host. Alternatively, a single VIB can carry updates for both the ESXi versions on the host and on the DPU device.

Table 1-1. Related Terminology

Term	Definition
VIB Metadata	An XML file (`descriptor.xml`) that describes the contents of the VIB. It also contains dependency information, textual descriptions, system requirements, and information about bulletins.
Standalone VIB	A VIB that is not included in a bulletin or component.

vSphere Lifecycle Manager does not consume and work with individual VIBs. VIBs must be further packaged into a higher-level construct, such as a base image, an add-on, and so on.

What Is a Bulletin?

The bulletin is a grouping of one or more VIBs. Bulletins are defined within the metadata of the VIB. You use bulletins, and not individual VIBs, to create vSphere Lifecycle Manager baselines, which you attach to inventory objects and use to update and upgrade ESXi hosts.

Table 1-2. Related Terminology

Term	Definition
Patch	A small software update that provides bug fixes or enhancements to the current version of the software. A patch groups one or more VIBs together to address a particular issue or to provide enhancements to the current version of the software.
Roll-up Bulletin	A collection of patches that are grouped to facilitate downloads and deployment.
Extension	A bulletin that defines a group of VIBs for adding an optional component to an ESXi host. An extension is usually provided by a third party. The third-party provider is also responsible for providing patches and updates for the extension.

What Are Software Components?

The component is the basic packaging construct for VIBs. VMware, OEMs, and third-party software providers deliver software in the form of components. The component is a bulletin with additional metadata specifying the name and the version of the component. Unlike the bulletin, the component is a logical grouping of VIBs that provides you with a complete and visible feature upon installation. Components can contain VIBs for the ESXi version on the server, ESXi version the DPU device of the server, if the server is DPU-backed, or for both of them.

VMware and OEMs do not deliver components independently. VMware bundles components together into fully functional and bootable ESXi base images. OEMs bundle components together into vendor add-ons. Third-party software vendors create and ship software, for example drivers or adapters, as independent components.

What Is a Base Image?

The base image is an ESXi image that VMware provides with every release of ESXi. The base image is a collection of components that is complete and can boot up a server. Base images have a user-readable name and a unique version that is updated with every major or minor release of ESXi.

The version of a base image corresponds to an ESXi release and uses the following naming format:

Release Type	Base Image Naming Example
General Availablity release	ESXi 8.0
Update release	ESXi 8.0 U1, ESXi 8.0 U2, and so on
Patch release	ESXi 8.0 a, ESXi 8.0 b, and so on
Security patch release	ESXi 8.0 sa, ESXi 8.0 sb, and so on
Patch release after an Update release	ESXi 8.0 U1 a, ESXi 8.0 U2 sa, and so on

In vSphere 8.0, base images can contain components and VIBs applicable to the ESXi version running on a DPU device. So, a single base image can contain software updates for both ESXi on the server and ESXi on the DPU device.

Base images are hosted and available in the VMware online depot. Additionally, you can download an ESXi installer ISO file and an offline bundle (ZIP file) that contains the ESXi version from customerconnect.vmware.com.

What Is a Vendor Add-On?

OEMs pack one or multiple components into a unit called an add-on. You use vendor add-ons to customize an ESXi image with OEM content and drivers.

The add-on is a collection of components that does not represent a complete, bootable image. You cannot use vendor add-ons on their own. To customize an ESXi release, you must add the vendor add-on to an ESXi base image. The combination of a vendor add-on and an ESXi base image is practically identical to the custom image that OEMs provide.

When combined with an ESXi base image, the add-on can add, update, or remove components that are part of the ESXi base image. In the vSphere Client, for each add-on available in the depot, you can view the list of components that it adds to an ESXi base image. Similarly, you can find information about the components that it removes from a base image.

In addition to custom ISO images and offline bundles, OEMs release ZIP files that contain only the vendor add-on, that is, the delta between the custom image and the ESXi base image. OEMs can release such add-on ZIP files at their discretion. The introduction of the concept of add-ons decouples the release cycle of OEMs from the release cycle of VMware. As a result, you can update vendor add-ons independently of updating the ESXi version of your hosts. Also, the vendor add-on decouples the OEM customization from the VMware stock image. As a result, you can combine software components more freely.

In vSphere 8.0, vendor add-ons support the ESXi software that runs on DPU devices.

Bulletins and Components in the vSphere Lifecycle Manager Depot

vSphere Lifecycle Manager can consume both bulletins and components.

If you use baselines and baseline groups to manage hosts and clusters, vSphere Lifecycle Manager reads and lists the software updates that are available in the vSphere Lifecycle Manager depot as bulletins. You can find the list of available bulletins on the **Updates** tab in the vSphere Lifecycle Manager home view.

If you use vSphere Lifecycle Manager images to manage hosts and clusters, you can only work with components and the related notions of add-ons and base images. You can find the list of the components, add-ons, and ESXi base images on the **Image Depot** tab in the vSphere Lifecycle Manager home view.

vSphere Lifecycle Manager Baselines and Images

vSphere Lifecycle Manager enables you to manage ESXi hosts and clusters with images or baselines. vSphere Lifecycle Manager baselines and vSphere Lifecycle Manager images are different in their essence, the way they work, and the features they support.

You use vSphere Lifecycle Manager baselines and baseline groups to perform the following tasks.

- Upgrade and patch ESXi hosts.
- Install and update third-party software on ESXi hosts.

You use vSphere Lifecycle Manager images to perform the following tasks.

- Install a desired ESXi version on all hosts in a cluster or on a standalone host.
- Install and update third-party software on all ESXi hosts in a cluster or on a standalone host.
- Update and upgrade the ESXi version on all hosts in a cluster or on a standalone host.
- Update the firmware of all ESXi hosts in a cluster or of a standalone host.
- Generate recommendations and use a recommended image for your cluster or host.
- Check the hardware compatibility of hosts and clusters against the VMware Compatibility Guide and the vSAN Hardware Compatibility List.

vSphere Lifecycle Manager Images

You use vSphere Lifecycle Manager images to apply software and firmware updates to the ESXi hosts in a cluster. Using a single image to manage all hosts in a cluster ensures cluster-wide host image homogeneity.

You can use various methods and tools to deploy ESXi hosts and maintain their software lifecycle. For example, you can upgrade hosts by using VMware vSphere® ESXi™ Image Builder CLI, esxcli, vSphere Auto Deploy. The different deployment and upgrade choices involve different workflows and require you to use different ESXi image formats. When you use vSphere Lifecycle Manager images, you follow one workflow and use the same ESXi image format for all software lifecycle-related operations: install, upgrade, update, and patching, which significantly simplifies the lifecycle management process.

Understanding vSphere Lifecycle Manager Images

A vSphere Lifecycle Manager image represents a desired software specification to be applied to all hosts in a cluster. When you set up a vSphere Lifecycle Manager image, you can define the full software stack that you want to run on the hosts in a cluster: the ESXi version, additional VMware software, vendor and third-party software, for example firmware and drivers.

A vSphere Lifecycle Manager image can consist of the following four elements:

- ESXi base image

  The base image contains an image of VMware ESXi Server and additional components, such as drivers and adapters that are necessary to boot a server. The base image is the only mandatory element in a vSphere Lifecycle Manager image. All other elements are optional.

- Vendor add-on

  The vendor add-on is a collection of software components that OEMs create and distribute. The vendor add-on can contain drivers, patches, and solutions.

- Firmware and drivers add-on

  The firmware and drivers add-on is a special type of vendor add-on designed to assist in the firmware update process. The firmware and drivers add-on contains firmware for a specific server type and corresponding drivers. To add a firmware and drivers add-on to your image, you must install the hardware support manager plug-in provided by the hardware vendor for the hosts in the respective cluster.

- Independent components

  The component is the smallest discrete unit in an image. The independent components that you add to an image contain third-party software, for example drivers or adapters.

You can set up a vSphere Lifecycle Manager image for a cluster during the creation of the cluster. Alternatively, for existing clusters that you mange with vSphere Lifecycle Manager baselines, you can switch from using baselines to using images at a later time.

Note If you switch to using images, you cannot revert to using baselines for that cluster. You can only move the hosts to a cluster that uses baselines.

The Desired State Model

The concept of images that vSphere Lifecycle Manager introduces is based on the Desired State model for managing ESXi hosts and clusters.

The desired state of an ESXi host represents both the target software and target configuration for the host as opposed to the software and configuration that it currently runs. The Desired State model is the idea of managing hosts and clusters by defining and applying a desired state instead of listing and following steps to change the current state.

vSphere Lifecycle Manager Baselines and Baseline Groups

You use baselines and baseline groups to update and upgrade the ESXi hosts in your environment. To start managing a cluster with baselines and baseline groups, you must skip setting up an image during the creation of the cluster.

Baselines

A baseline is a grouping of multiple bulletins. You can attach a baseline to an ESXi host and check the compliance of the host against the associated baseline.

Baselines can be classified according to different criteria.

- Depending on the type of content, baselines are patch baselines, extension baselines, and upgrade baselines.

  Patch and extension baselines contain bulletins of the respective kind. Upgrade baselines contain ESXi images.

- Depending on how the update content is selected, baselines are fixed and dynamic.
- Depending on how they are created and managed, baselines are predefined, recommendation, or custom baselines.

Baseline Groups

A baseline group is a collection of non-conflicting baselines. You can attach the entire baseline group to an inventory object to check the compliance status of the object against all the baselines in the group as a whole.

You can combine custom baselines with any of the predefined baselines to create baseline groups.

Host baseline groups can contain a single upgrade baseline, and various patch and extension baselines.

To update or upgrade ESXi hosts by using baselines or baseline groups, you must first attach the baselines or baselines group to an inventory object.

Although you can attach baselines and baseline groups to individual objects, a more efficient method is to attach them to container objects, such as folders, vApps, clusters, and data centers. Individual vSphere objects inherit baselines attached to the parent container object. Removing an object from a container removes the inherited baselines from the object.

For more information about creating and managing baselines and baseline groups, see Types of vSphere Lifecycle Manager Baselines and Baseline Groups.

What Is the Difference Between vSphere Lifecycle Manager Images and Baselines

A vSphere Lifecycle Manager baseline is a collection of bulletins. A vSphere Lifecycle Manager image is a combination of components, vendor add-on, and an ESXi base image. Some differences exist between the operations that you can perform on clusters that you manage with a vSphere Lifecycle Manager image and the operations on clusters that you manage with vSphere Lifecycle Manager baselines.

Operation	Baselines	Images
Distribution	Bulletins are distributed through online depots and as offline bundles. You can import and use ISO images to create upgrade baselines.	Base image, vendor add-ons, and components are distributed through online depots and as offline bundles. You cannot use ISO images to set up a vSphere Lifecycle Manager image for a cluster.
Validation	Not supported. You do not validate a baseline before applying the updates to the hosts. You can only perform a remediation pre-check.	Supported. You can validate a vSphere Lifecycle Manager image to check if it is applicable to all hosts in the cluster. You can also perform a remediation pre-check.
Import/Export	You can create a custom baseline and attach it to different objects in the same vCenter Server instance. You cannot export baselines and distribute them across vCenter Server instances.	You can export an image and use it to manage other clusters in the same or in a different vCenter Server instance. Images are portable across vCenter Server instances. You can export an image as an ISO or JSON file, but you can only import images that are in a JSON format.
Compliance checks	With baselines, you can check the compliance of an object against a single or against multiple baselines.	With vSphere Lifecycle Manager images, you can check the compliance of the hosts against a single image. To check the compliance against another image, you must first set up the new image.

Operation	Baselines	Images
Staging	Supported. You can stage updates to the hosts before actually installing them.	Supported. You can stage an image to a cluster or a host in the cluster before remediation. Staging reduces ESXi downtime.
Remediation	With vSphere Lifecycle Manager baselines, you can remediate an object against a single baseline or against multiple baselines. So, with a single operation, you can patch and upgrade a host. However, vSphere Lifecycle Manager baselines list the updates to be applied to hosts, but the remediation result is not always predictable, because ESXi image on the hosts might change after remediation.	With vSphere Lifecycle Manager images, you can add, remove, or modify the components in the image that you use for a cluster. When you remediate the hosts against the new image, all modified components are applied to the host. So, you can upgrade and patch a host with a single remediation operation. vSphere Lifecycle Manager images define the precise image to be applied to the hosts after remediation. No deviation from the defined image is possible after remediation. vSphere Lifecycle Manager does not allow solutions to push VIBs to the hosts.
Firmware updates	Not supported.	Supported. With vSphere Lifecycle Manager images, firmware updates are carried out through firmware and drivers add-ons, which you add to the image that you use to manage a cluster. Updating firmware with images requires an OEM-provided hardware support manager plug-in, which integrates with vSphere Lifecycle Manager.
Hardware compatibility checks	Not supported.	Supported You can check the hardware compatibility of the hosts in a cluster against the VMware Compatibility Guide (VCG). You can also check the compatibility of all hosts in a vSAN-enabled cluster against the vSAN Hardware Compatibility List (vSAN HCL).
Software recommendations	Limited support. Software recommendations are only available for vSAN clusters in the form of recommendation baselines.	Supported. Based on the hardware of the hosts in the cluster, you get recommendations about available and applicable ESXi updates or upgrades.

Operation	Baselines	Images
vCenter Server /Datacenter-level operations	With vSphere Lifecycle Manager baselines, you can trigger any of the main operations at the vCenter Server or data center level.	With vSphere Lifecycle Manager images, you cannot operate at a vSphere Lifecycle Manager or data center level.
Virtual machine management	You can upgrade the VMware Tools and virtual hardware versions of the virtual machines in a cluster that you manage with vSphere Lifecycle Manager baselines.	You can upgrade the VMware Tools and virtual hardware versions of the virtual machines in a cluster that you manage with vSphere Lifecycle Manager images.
Update Manager Download Service (UMDS)	Supported.	Supported.
Remote Office/Branch Office (ROBO) support	Not provided. Although no specific optimization exists for ROBO deployments, you can still use baselines and baseline groups with ROBO clusters.	Provided. With vSphere Lifecycle Manager images, you can set up a local depot and use it in ROBO environments. For more information, see Manage Depot Overrides for a Cluster or a Standalone Host.
REST APIs	Not available.	Available.
Support for DPU devices	Not provided. You cannot use baselines for clusters that contain hosts with DPU devices.	Provided To manage a cluster of DPU-backed hosts, you can only use vSphere Lifecycle Manager images. All vSphere Lifecycle Manager operations that work for updating the ESXi version on the host also deliver updates to the ESXi version on the DPU device on the host.

What Are the Requirements for Using vSphere Lifecycle Manager

Depending on whether you want to use baselines or images for software lifecycle management, you must comply with a different set of requirements. To achieve your goals, you must also know the specifics in behavior and limitations that vSphere Lifecycle Manager has.

Table 1-3. Requirements for Using vSphere Lifecycle Manager

Scenario	Requirements
Using a single image to manage a cluster.	■ All ESXi hosts in the cluster must be of version 7.0 and later. ■ All ESXi hosts in the cluster must be stateful. A stateful install is one in which the host boots from a disk. ■ All ESXi hosts in the cluster must be from the same vendor and with identical hardware. Different generations and models of servers need different software drivers, which implies that you must set up different vSphere Lifecycle Manager images to manage each generation or model. However, with vSphere Lifecycle Manager, you use one single image for the entire cluster. Also, vSphere Lifecycle Manager does not detect and handle the hardware differences between the hosts in the cluster. You can use a vSphere Lifecycle Manager image to manage a heterogeneous cluster only if the vSphere Lifecycle Manager image for the cluster includes vendor customization, for example a vendor or firmware add-on, that can address and handle the hardware differences across the hosts in the cluster, which is a rare scenario. ■ If you want to use DPU devices for network acceleration, all hosts in the cluster must have a DPU device from the same vendor and of the same model. You cannot add a host without a DPU device to a cluster of DPU-backed hosts. ■ The cluster must include only integrated solutions. For example: ■ VMware vSAN™ ■ VMware vSphere® High Availability (HA) ■ vSphere IaaS control plane ■ NSX
Using a single image to manage a standalone host.	■ The standalone ESXi host must be of version 7.0 and later. ■ The standalone ESXi host must be stateful. A stateful install is one in which the host boots from a disk. ■ The host must include only integrated solutions. For example, the witness host for a vSAN stretch cluster must be a standalone host. For more information, see the *vSAN Planning and Deployment* documentation and vSAN Clusters and vSphere Lifecycle Manager.

Table 1-3. Requirements for Using vSphere Lifecycle Manager (continued)

Scenario	Requirements
Using baselines and baseline groups to manage a cluster or a host.	■ To use baselines for ESXi host patching operations, vSphere Lifecycle Manager works with ESXi 6.7, ESXi 7.0, and ESXi 8.0. ■ To use baselines for ESXi host upgrade operations, vSphere Lifecycle Manager works withESXi 6.7, ESXi 7.0, and their respective Update releases.
Switching from using baselines to using a single image to manage a cluster or a host.	■ The cluster or the standalone host must meet the requirements for using an image. ■ The cluster or the standalone host must be eligible for the transition. For more information about the **Check cluster's eligibility to be managed with a single image** and **Check host's eligibility to be managed with a single image** tasks, see Cluster or Standalone Host Eligibility to Use vSphere Lifecycle Manager Images.
Upgrading virtual machine hardware and VMware Tools	For VMware Tools and virtual machine hardware upgrade operations, vSphere Lifecycle Manager works with ESXi 6.7, ESXi 7.0, and ESXi 8.0.

Required Privileges for Using vSphere Lifecycle Manager and vSphere Configuration Profiles

To configure vSphere Lifecycle Manager settings and to use successfully vSphere Lifecycle Manager baselines and images, you must have the proper privileges. Similarly, you need the proper privileges to use vSphere Configuration Profiles.

You can assign vSphere Lifecycle Manager and vSphere Configuration Profiles privileges to different roles in the vSphere Client.

vSphere Lifecycle Manager Privileges For Using Images

When you use vSphere Lifecycle Manager images, you need a different set of privileges for each task.

Table 1-4. VMware vSphere vSphere Lifecycle Manager Privileges For Using Images

Task	Privilege in the vSphere Client	Privilege in the API
Set Up Image	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Write** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read**	■ `VcIntegrity.lifecycleSoftwareSpecification.Read` ■ `VcIntegrity.lifecycleSoftwareSpecification.Write` ■ `VcIntegrity.lifecycleSettings.Read`
Import Image	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Write** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read** ■ **VMware vSphere Lifecycle Manager .Upload File.Upload upgrade images and offline bundles**	■ `VcIntegrity.lifecycleSoftwareSpecification.Read` ■ `VcIntegrity.lifecycleSoftwareSpecification.Write` ■ `VcIntegrity.lifecycleSettings.Read` ■ `VcIntegrity.FileUpload.com.vmware.vcIntegrity.ImportFile`
Export Image	**VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read**	`VcIntegrity.lifecycleSoftwareSpecification.Read`
Edit Image	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Write** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read**	■ `VcIntegrity.lifecycleSoftwareSpecification.Read` ■ `VcIntegrity.lifecycleSoftwareSpecification.Write` ■ `VcIntegrity.lifecycleSettings.Read`
Work with Recommendations	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Write** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read**	■ `VcIntegrity.lifecycleSoftwareSpecification.Read` ■ `VcIntegrity.lifecycleSoftwareSpecification.Write` ■ `VcIntegrity.lifecycleSettings.Read`

Table 1-4. VMware vSphere vSphere Lifecycle Manager Privileges For Using Images (continued)

Task	Privilege in the vSphere Client	Privilege in the API
Work with Depot	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Write**	■ `VcIntegrity.lifecycleSoftwareSpecification.Read` ■ `VcIntegrity.lifecycleSoftwareSpecification.Write`
Manage Depot Overrides	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Write**	■ `VcIntegrity.lifecycleSoftwareSpecification.Read` ■ `VcIntegrity.lifecycleSoftwareSpecification.Write`
Check Compliance	**VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read**	`VcIntegrity.lifecycleSoftwareSpecification.Read`
Run Remediation Pre-Check	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: General Privileges.Read** ■ **VMware vSphere Lifecycle Manager.ESXi Health Perspectives.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Remediation Privileges.Read**	■ `VcIntegrity.lifecycleGeneral.Read` ■ `VcIntegrity.lifecycleHealth.Read` ■ `VcIntegrity.lifecycleSoftwareRemediation.Read`
Remediate Against an Image	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: General Privileges.Read** ■ **VMware vSphere Lifecycle Manager.ESXi Health Perspectives.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Remediation Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Remediation Privileges.Write** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read**	■ `VcIntegrity.lifecycleGeneral.Read` ■ `VcIntegrity.lifecycleHealth.Read` ■ `VcIntegrity.lifecycleSoftwareRemediation.Read` ■ `VcIntegrity.lifecycleSoftwareRemediation.Write` ■ `VcIntegrity.lifecycleSettings.Read`
Edit Remediation Settings	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Write**	■ `VcIntegrity.lifecycleSettings.Read` ■ `VcIntegrity.lifecycleSettings.Write`

Table 1-4. VMware vSphere vSphere Lifecycle Manager Privileges For Using Images (continued)

Task	Privilege in the vSphere Client	Privilege in the API
Update Firmware	■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Read** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Privileges.Write** ■ **VMware vSphere Lifecycle Manager.Lifecycle Manager: Settings Privileges.Read**	■ `VcIntegrity.lifecycleSoftwareSpecification.Read` ■ `VcIntegrity.lifecycleSoftwareSpecification.Write` ■ `VcIntegrity.lifecycleSettings.Write`
View Hardware Compatibility	**VMware vSphere Lifecycle Manager.Lifecycle Manager: Hardware Compatibility Privileges.Access Hardware Compatibility**	`VcIntegrity.HardwareCompatibility.Read`
Stage an Image	**VMware vSphere Lifecycle Manager.Lifecycle Manager: Image Remediation Privileges.Write**	`VcIntegrity.lifecycleSoftwareRemediation.Write`

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

vSphere Lifecycle Manager Privileges For Using Baselines

Each of the vSphere Lifecycle Manager privileges that you need to use baselines and baseline groups covers a distinct functionality.

Table 1-5. VMware vSphere Lifecycle Manager Privileges For Using Baselines

Task	Privilege in the vSphere Client	Privilege in the API	Description
Configure	**Configure.Configure Service**	`VcIntegrity.General.com.vmware.vcIntegrity.Configure`	Configure the vSphere Lifecycle Manager service and the scheduled patch download task.
Manage Baseline	**Manage Baselines.Attach Baseline**	`VcIntegrity.Baseline.com.vmware.vcIntegrity.AssignBaselines`	Attach baselines and baseline groups to objects in the vSphere inventory.
	Manage Baselines.Manage Baselines	`VcIntegrity.Baseline.com.vmware.vcIntegrity.ManageBaselines`	Create, edit, or delete baselines and baseline groups.
Manage Patches and Upgrades	**Manage Patches and Upgrades.Remediate to Apply Patches, Extensions, and Upgrades**	`VcIntegrity.Updates.com.vmware.vcIntegrity.Remediate`	Remediate virtual machines and hosts to apply patches, extensions, or upgrades. In addition, this privilege allows you to view the compliance status of objects.

Table 1-5. VMware vSphere Lifecycle Manager Privileges For Using Baselines (continued)

Task	Privilege in the vSphere Client	Privilege in the API	Description
	Manage Patches and Upgrades .Scan for Applicable Patches, Extensions, and Upgrades	`VcIntegrity.Updates.com.vmware.vcIntegrity.Scan`	Scan virtual machines and hosts to search for applicable patches, extensions, or upgrades.
	Manage Patches and Upgrades .Stage Patches and Extensions	`VcIntegrity.Updates.com.vmware.vcIntegrity.Stage`	Stage patches or extensions to hosts. In addition, this privilege allows you to view the compliance status of hosts.
	Manage Patches and Upgrades .View Compliance Status	`VcIntegrity.Updates.com.vmware.vcIntegrity.ViewStatus`	View baseline compliance information for an object in the vSphere inventory.
Upload File	**Upload File.Upload upgrade images and offline bundles**	`VcIntegrity.FileUpload.com.vmware.vcIntegrity.ImportFile`	Upload upgrade images and offline patch bundles.

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

Required Privileges for Using vSphere Configuration Profiles

When you use vSphere Configuration Profiles, you need a different set of privileges for each task.

Table 1-6. Required Privileges For Using vSphere Configuration Profiles

Task	Privilege in the vSphere Client	Privilege in the API	Description
Create Cluster with vSphere Configuration Profiles enabled	**Host.Inventory.CreateCluster**	`Host.Inventory.CreateCluster`	Create a cluster along with its initial configuration.
View Host Settings in the Cluster Configuration Check Cluster Compliance View Compliance Results Run Remediation Pre-Check View Remediation Pre-Check Results View Draft Pre-Check Results	**VMware vSphere Lifecycle Manager .Desired Configuration Management Privileges.Read-only access to desired configuration management platform**	`VcIntegrity.ClusterConfiguration.View`	View the draft configuration document, current configuration settings, compliance reports, and pre-check reports.
Remediate a Cluster Against the Desired Cluster Configuration	**VMware vSphere Lifecycle Manager .Desired Configuration**	`VcIntegrity.ClusterConfiguration.Remediate`	Remediate a cluster against the draft configuration or transition

Table 1-6. Required Privileges For Using vSphere Configuration Profiles (continued)

Task	Privilege in the vSphere Client	Privilege in the API	Description
Transition to vSphere Configuration Profiles	**Management Privileges.Remediate cluster to the desired configuration.**		a cluster to the desired configuration.
Export a Configuration or Configuration Schema	**VMware vSphere Lifecycle Manager .Desired Configuration Management Privileges.Export desired cluster configuration**	`VcIntegrity.ClusterConfiguration.Export`	Export the desired cluster configuration document.
Extract a Configuration Document from a Reference Host Create a Draft Configuration for a Cluster Import a Configuration	**VMware vSphere Lifecycle Manager .Desired Configuration Management Privileges.Modify desired cluster configuration.**	`VcIntegrity.ClusterConfiguration.Modify`	Modify the desired cluster configuration by crating a draft configuration, extracting a configuration document from a reference host, or importing a configuration.

The vSphere Lifecycle Manager Depot

2

The vSphere Lifecycle Manager depot is the source of software updates for vSphere Lifecycle Manager. Conceptually, the vSphere Lifecycle Manager depot represents all software available for consumption to vSphere Lifecycle Manager.

The vSphere Lifecycle Manager depot is a local depot on the vCenter Server machine. This local depot contains software updates downloaded from the online depots that you configure vSphere Lifecycle Manager to use. You can also manually import updates into the vSphere Lifecycle Manager depot. You can work with vSphere Lifecycle Manager only if the vSphere Lifecycle Manager depot contains software packages, for example, ESXi base images, vendor add-ons, third-party components, and legacy patches and updates.

How Do Software Updates Go to the vSphere Lifecycle Manager Depot

You control how the vSphere Lifecycle Manager depot gets populated with software. You can configure vSphere Lifecycle Manager to download updates from online depots. In environments without access to the Internet, you can use the Update Manager Download Service (UMDS) and configure vSphere Lifecycle Manager to download software from a UMDS-created shared repository. Alternatively, you can use offline depots to import updates into the vSphere Lifecycle Manager depot manually.

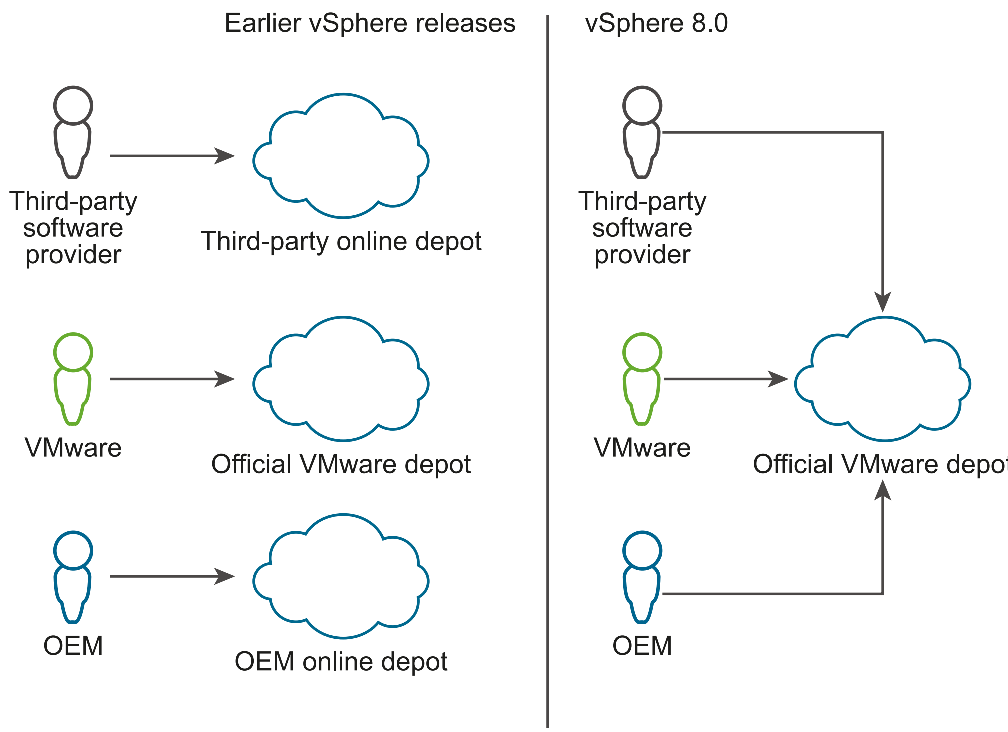
What Is an Online Depot and What Is the Default VMware Online Depot

VMware, OEMs, and third-party software providers create and ship their software updates in a well-defined `xml` file structure, which is called a software depot. Depending on the distribution format of the updates, software depots can be online and offline.

An online depot is the hosted version of the software updates that VMware, OEMs, and third-party software providers ship. You enable vSphere Lifecycle Manager to access an online depot by providing a URL to that depot. vSphere Lifecycle Manager is preconfigured to download updates from one online depot, the default VMware online depot.

The VMware Online Depot

The default online depot that VMware provides hosts ESXi base images, vendor add-ons, ESXi-compatible I/O device drivers certified by VMware, and async VMware Tools releases. All software that you need to install, update, or customize the ESXi version of your hosts is available in the official VMware online depot. You don't need to work with separate online depots to access OEM and third-party software updates.



Note Firmware updates are not hosted in the VMware depot. To perform firmware updates, you must install the hardware support manager plug-in that your hardware vendor provides. The plug-in gives you access to depots that contain the necessary firmware and related drivers updates.

You can configure vSphere Lifecycle Manager to also access and use other online depots besides the VMware online depot, for example third-party depots that contain additional components such as CIM modules. However, working with additional third-party depots and independent components is rarely necessary. In most cases, the vendor add-ons that are available in the official VMware depot provide full OEM customization for ESXi.

vSphere Lifecycle Manager downloads to the local vSphere Lifecycle Manager depot the content from all the online depots that you configure it to use.

Synchronization

Synchronization is the process during which vSphere Lifecycle Manager downloads the contents of the online depots that you configure it to use to the local vSphere Lifecycle Manager depot. During synchronization, only software metadata is downloaded. The actual payloads are downloaded when they are needed, for example during staging or remediation. When you deploy vCenter Server, vSphere Lifecycle Manager synchronizes with the official

VMware online depot automatically. After the initial synchronization, you can schedule a download task to run at regular intervals or you can initiate a download task manually.

What Is an Offline Depot

An offline depot, also called an offline bundle, is a ZIP file that you download from the Internet or copy from a media drive and you save on a local or a shared network drive. You then can import the offline bundle to the vSphere Lifecycle Manager depot.

All software updates hosted in the official VMware online depot are also available as offline bundles, which you can download from my.vmware.com. You can also download offline bundles from the VMware website or from the websites of third-party vendors.

In addition to distributing an `offline.zip` file, or offline bundle, and a custom ISO image, OEMs distribute an `Add-on.zip` file that contains the delta between the OEM custom image and the respective base image that VMware provides. For more information about OEM add-ons, see Software Packaging Units That vSphere Lifecycle Manager Can Consume.

Import

Import is the operation through which you upload the contents of an offline bundle into the vSphere Lifecycle Manager depot. During an import operation, both the software metadata and the actual payloads are downloaded into the vSphere Lifecycle Manager depot. In addition to importing offline bundles, you can also import ISO images to the vSphere Lifecycle

Manager depot. You can then use the ISO images to create upgrade baselines. You cannot use an ISO image for clusters that you manage with a vSphere Lifecycle Manager image.

Software Deliverables and Their Corresponding Distribution Formats

Software Vendor	Software Deliverable	Software Distribution Format
VMware	Base images	■ The default VMware online depot ■ Offline bundle ■ ISO image
OEMs	Add-ons	■ The default VMware online depot ■ Offline bundle ■ Add-on ZIP file ■ ISO image
Third-party software providers	Components	For device drivers that are certified by VMware: ■ The default VMware online depot ■ Offline bundle For other third-party software that is verified and certified by OEMs, for example I/O filters, CIM module: ■ An online depot ■ Offline bundle

vSphere Lifecycle Manager Download Sources

The vSphere Lifecycle Manager download source is the place from which vSphere Lifecycle Manager downloads software updates.

If you configure vSphere Lifecycle Manager to use the Internet as its download source, then the download sources are practically all online depots that you use with vSphere Lifecycle Manager.

You can also configure vSphere Lifecycle Manager to use a UMDS shared repository as its download source. Using a UMDS repository is appropriate in vCenter Server deployments without access to the Internet. When you configure vSphere Lifecycle Manager to use a UMDS repository, the synchronization of update metadata is not triggered immediately. The metadata is downloaded according to the configured download schedule or when you initiate the download. When you use a UMDS repository as a download source for vSphere Lifecycle Manager, only the metadata of the updates is downloaded and stored in the vSphere Lifecycle Manager depot. The actual payload is downloaded during staging or remediation.

Depot Overrides

In ROBO scenarios, you can configure vSphere Lifecycle Manager to use a local depot with updates for a particular cluster instead of the depots that all clusters in that vCenter Server instance use by default.

For more information, see Manage Depot Overrides for a Cluster or a Standalone Host.

Read the following topics next:

- Browsing the vSphere Lifecycle Manager Depot
- Working With the vSphere Lifecycle Manager Depot
- Configuring the vSphere Lifecycle Manager Download Sources
- Add a New Download Source
- Configure the vSphere Lifecycle Manager Automatic Download Task
- Installing, Setting Up, and Using the Update Manager Download Service

Browsing the vSphere Lifecycle Manager Depot

You can use the vSphere Client to view and browse the contents of the vSphere Lifecycle Manager depot.

You can view the vSphere Lifecycle Manager depot in the vSphere Lifecycle Manager home view. The contents of the vSphere Lifecycle Manager depot are displayed on three different tabs: **Image Depot**, **Updates**, and **Imported ISOs**.

Image Depot

On the **Image Depot** tab, you can view all VMware base images, vendor add-ons, and components that are available in the vSphere Lifecycle Manager depot.

You can use the **ESXi Versions**, **Vendor Addons**, and **Component** links at the top of the pane for easier navigation through the lists.

The **ESXi Versions** list contains all base images available in the depot together with information about the version, release date, and category for each image. When you select an image from the list, an information panel appears on the right. The panel displays a list of all components that the base image applies to a host upon remediation.

The **Vendor Addons** list contains all vendor addons available in the depot together with information about the version, release date, and category for each addon. When you select an add-on from the list, an information panel appears on the right. The panel displays information about the components that the add-on applies to the host and the components that the add-on removes from a host upon remediation.

The **Component** list contains all components that are available in the depot together with information about the version, release date, and category for each component. When you select a component from the list, an information panel appears on the right. The panel displays information about the VIBs that the component contains.

You can filter the **Component** list so that it displays only independent components or all components available in the vSphere Lifecycle Manager depot. Independent components are components that are not part of a vendor add-on.

You use the ESXi images, vendor add-ons, and components visible on the **Image Depot** tab to set up images that you can use to manage hosts in clusters collectively.

Updates

On the **Updates** tab, you can see all components available in the vSphere Lifecycle Manager depot as bulletins. You can use the **Filter by Baseline** drop-down menu to view only the bulletins that are part of a particular baseline.

When you select a bulletin from the list, additional information appears below the bulletins list. In the bottom pane, you see information about the baselines that include the selected bulletin.

You use the bulletins visible on the **Updates** tab to create baselines and baseline groups.

Because the official VMware depot hosts certified partner content in addition to VMware content, the **Updates** tab displays a broader set of OEM bulletins, for example vendor add-ons and VMware-certified device drivers. Some of these bulletins might have dependencies that must be pulled into the baselines that you create, so that the remediation against those baselines is successful. As a best practice, always consult the KB article for an individual bulletin to find information about its deployment specfics and reqired dependencies before including the bulletin in your baselines.

Starting with vSphere 7.0, some changes are also introduced in the way VMware content is packaged. As a result, you might see additional bulletins on the **Updates** tab at patch and update releases. Those bulletins are usually of the Enhancement or BugFix category. When you include those bulletins in a baseline, you might need to also include a base ESXi bulletins in that baseline. As a best practice, to ensure successful application of patches and updates, always include the appropriate rollup bulletin into your baselines. You can use the **Show only rollup updates** toggle switch that is on the **Updates** tab to filter the list of bulletins.

Imported ISOs

On the **Imported ISOs** tab, you can see the ISO images that you import and make available to vSphere Lifecycle Manager.

You use the ISO images visible on the **Imported ISOs** tab to create upgrade baselines. You cannot use an ISO image for clusters configured to use a single vSphere Lifecycle Manager image.

Note ISO images are not distributed through any online or offline depot, they are a separate software distribution format. As a result, they cannot become available in the vSphere Lifecycle Manager depot through synchronization or the regular import operation that you perform to import offline bundles (ZIP files) to the depot. To make an ISO image available to vSphere Lifecycle Manager, you must trigger the **Import ISO** operation. For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot

Working With the vSphere Lifecycle Manager Depot

The vSphere Lifecycle Manager synchronizes to its download source regularly and automatically. But you can change the contents of the vSphere Lifecycle Manager depot by manually importing or deleting updates or ISO images or by triggering synchronization at a convenient time.

Import Updates to the vSphere Lifecycle Manager Depot

You can use an offline bundle in ZIP format and import updates to the vSphere Lifecycle Manager depot manually. When you import offline bundles, you add both the update metadata and actual payload to the vSphere Lifecycle Manager depot.

You use the import option to populate the vSphere Lifecycle Manager depot with updates from an offline bundle. Apart from the legacy patches and extensions, an offline bundle can also contain an ESXi base image, a vendor add-on, or third-party software, for example, asynchronous drivers specific to the OEM hardware requirements. For more information about base images, vendor add-ons, and components, see Software Packaging Units That vSphere Lifecycle Manager Can Consume.

If you want to use vSphere Lifecycle Manager baselines, you can import offline bundles that contain patches and extensions for hosts that run ESXi 6.7 and later. In that case, you can use the contents of the offline bundle only for host patching operations. If you import an OEM offline bundle that contains an ESXi image of a version earlier than 7.0, you cannot use the image for upgrade operations. To create upgrade baselines, you need an ISO image. For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.

If you want to use vSphere Lifecycle Manager images, you can import offline bundles that contain software for hosts that run ESXi 7.0 and later. In that case, you can use the contents of the offline bundle to set up vSphere Lifecycle Manager images, which you can use to upgrade a standalone host or multiple ESXi hosts collectively.

Prerequisites

- Verify that the updates that you import are in ZIP format.
- Required privileges: **VMware vSphere Lifecycle Manager.Upload File.Upload File**.

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 Select **Actions > Import Updates** at the top of the vSphere Lifecycle Manager home view.

   The **Import Updates** dialog box opens.

3 Enter a URL or browse to an offline bundle in ZIP format on your local machine.

   If the upload fails, check whether the structure of the ZIP file is correct and whether the vSphere Lifecycle Manager network settings are set up correctly.

4 Click **Import**.

   The Import updates task appears in the **Recent Tasks** pane.

Results

You imported updates to the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager automatically generates new image recommendations for the clusters or hosts that already have generated recommended images. However, if the imported updates are solution components only, vSphere Lifecycle Manager does not generate new recommendations automatically.

You can view the imported patches and extension on the **Updates** tab in the vSphere Lifecycle Manager home view.

You can view the imported ESXi images, vendor add-ons, and additional components on the **Image Depot** tab in the vSphere Lifecycle Manager home view.

Import an ISO Image to the vSphere Lifecycle Manager Depot

You import ESXi images in ISO format to the vSphere Lifecycle Manager local depot, so that you can create upgrade baselines, which you use for host upgrade operations.

You can use ESXi `.iso` images to upgrade ESXi 6.7.x hosts and ESXi 7.0.x hosts to ESXi 8.0.

With vSphere Lifecycle Manager 8.0, you cannot perform ESXi upgrades to version 7.0 or 6.7.

ISO images can only be used with vSphere Lifecycle Manager baselines. You cannot use an ISO image to upgrade the hosts in a cluster that uses a single image.

To upgrade hosts, use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-7.0.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder. You can also use ISO images created and distributed by OEMs.

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Upload File**

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Imported ISOs** tab, click **Import ISO**

3 In the **Import ISO** dialog box, select an image.

   - Click the **Browse** button to import an ESXi image from your local system.
   - Enter an URL address to import an ESXi image that is not on your local system.

   Local images are imported immediately, whereas importing images from a URL takes some time.

4 Click **Import**.

Results

The ISO image that you uploaded appears in the list of images. You can view information about the ESXi image, such as product, version, and build details, vendor, acceptance level, and creation date.

What to do next

Create a host upgrade baseline.

Delete an ISO Image from the vSphere Lifecycle Manager Depot

If you do not need an ESXi image, you can delete it from the vSphere Lifecycle Manager depot.

Unlike components and bulletins, which you cannot delete from the vSphere Lifecycle Manager depot, the ISO images that you import in the depot can be deleted when you no longer need them .

Prerequisites

- Verify that the ISO image that you want to delete is not part of any baseline. You cannot delete images that are included in a baseline.
- Delete any baseline that contains the ISO image that you want to delete.

Procedure

1. Navigate to the vSphere Lifecycle Manager home view.
   a. In the vSphere Client, select **Menu > Lifecycle Manager**.
   b. Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Imported ISOs** tab, select an image from the list and click **Delete**.

   Note If you try to delete an ESXi image that is used in a baseline, the operation fails with an error message.
3. Click **Yes** to confirm the deletion.

Results

The ISO image is deleted and no longer available.

Synchronize the vSphere Lifecycle Manager Depot

Instead of waiting for the predefined download task to run as scheduled, you can update your local vSphere Lifecycle Manager depot immediately.

At regular configurable intervals, vSphere Lifecycle Manager downloads updates from the configured download sources. The download sources can be online depots or a UMDS-created shared repository.

Regardless of the download schedule, you can initiate synchronization between the vSphere Lifecycle Manager depot and the configured download sources. Similar to scheduled synchronization, when you initiate synchronization manually, vSphere Lifecycle Manager downloads software from all online depots that you configured it to use. For more information about configuring the vSphere Lifecycle Manager download sources, see Configuring the vSphere Lifecycle Manager Download Sources.

During synchronization, vSphere Lifecycle Manager downloads only the update metadata, the actual payloads are downloaded during staging or remediation.

Procedure

1. Navigate to the vSphere Lifecycle Manager home view.
   a. In the vSphere Client, select **Menu > Lifecycle Manager**.
   b. Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 Select **Actions > Sync Updates** at the top of the vSphere Lifecycle Manager home view.

The Sync updates task appears in the **Recent Tasks** pane.

Results

You downloaded updates to the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager automatically generates new image recommendations for the clusters that already have generated recommended images. However, if the updates are related to downloading solution components only, vSphere Lifecycle Manager does not generate new recommendations automatically.

You can view the downloaded patches and extension on the **Updates** tab in the vSphere Lifecycle Manager home view.

You can view the downloaded ESXi images, vendor add-ons, and components on the **Image Depot** tab in the vSphere Lifecycle Manager home view.

Configuring the vSphere Lifecycle Manager Download Sources

You can configure vSphere Lifecycle Manager to download software updates for ESXi hosts either from the Internet or from a shared repository of UMDS data.

vSphere Lifecycle Manager downloads only the metadata and not the actual binary payload of the updates. Downloading the metadata saves disk space and network bandwidth. The availability of regularly updated metadata in the vSphere Lifecycle Manager depot lets you perform compliance checks on hosts at any time.

Whatever the download source, vSphere Lifecycle Manager downloads the following types of information:

- Metadata about all ESXi 6.x updates regardless of whether you have hosts of such versions in your environment.
- Metadata about all ESXi 7.x updates regardless of whether you have hosts of such versions in your environment.
- Patch recalls for ESXi 6.x hosts.

  vSphere Lifecycle Manager supports the recall of patches for hosts that are running ESXi6.7 or later. A patch is recalled when it has problems or potential issues. After you scan the hosts in your environment, vSphere Lifecycle Manager alerts you if the recalled patch has been installed on any host. Recalled patches cannot be installed on hosts with vSphere Lifecycle Manager. vSphere Lifecycle Manager deletes all the recalled patches from the vSphere Lifecycle Manager depot. After a patch that fixes the problem is released, vSphere Lifecycle Manager downloads the new patch to its depot. If you have already installed the problematic patch, vSphere Lifecycle Manager notifies you that a fix is available and prompts you to apply the new patch.

Downloading host patches from the VMware website is a secure process.

- Patches are cryptographically signed with the VMware private keys. Before you try to install a patch on a host, the host verifies the signature. This signature enforces the end-to-end protection of the patch itself and can also address any concerns about downloading the patch.
- vSphere Lifecycle Manager downloads the patch metadata and patch binaries over SSL connections. vSphere Lifecycle Manager verifies both the validity of the SSL certificates and the common name in the certificates. The common name in the certificates must match the names of the servers from which vSphere Lifecycle Manager downloads the patches. vSphere Lifecycle Manager downloads the patch metadata and binaries only after successful verification of the SSL certificates.

Download Sources

If your deployment system is connected to the Internet, you can use the default settings and links for downloading updates to the vSphere Lifecycle Manager depot. You can also add URL addresses to download third-party software, for example drivers.

If your deployment system is not connected to the Internet, you can use a shared repository after downloading the upgrades, patches, and extensions by using Update Manager Download Service (UMDS).

For more information about UMDS, see Installing, Setting Up, and Using the Update Manager Download Service.

The default configuration is for the vSphere Lifecycle Manager to download information directly from the Internet. However, you can change the download source at any time. Changing the download source from a shared repository to the Internet and the reverse is a change in the vSphere Lifecycle Manager configuration. The two options are mutually exclusive. You cannot download updates from the Internet and a shared repository at the same time.

By default, vSphere Lifecycle Manager is configured to use the official VMware online depot as a download source. When you deploy vCenter Server, synchronization to the official VMware depot is triggered automatically. When you change the default download source, synchronization to the new download source is not triggered automatically. The synchronization task runs as per its schedule. To download new data, you must run the **VMware vSphere Lifecycle Manager Update Download** task or trigger synchronization manually.

The **VMware vSphere Lifecycle Manager Update Download** task is a scheduled task that runs at regular intervals. You can change the schedule, and you can also trigger the **VMware vSphere Lifecycle Manager Update Download** task independently of its schedule.

If the **VMware vSphere Lifecycle Manager Update Download** task is running when you apply the new configuration settings, the task continues to use the old settings until it finishes. The next time the download task starts, vSphere Lifecycle Manager uses the new settings.

Using a Proxy Server

You cannot configure vSphere Lifecycle Manager to use a proxy server on its own. vSphere Lifecycle Manager uses the proxy settings of thevCenter Server instance where it runs.

Configure vSphere Lifecycle Manager to Use the Internet as a Download Source

If your deployment system is connected to the Internet, you can configure vSphere Lifecycle Manager to directly download ESXi images, vendor add-ons, and other components from the configured online depots to the local vSphere Lifecycle Manager depot.

The Internet is the default download source for vSphere Lifecycle Manager. Downloading takes place at configurable regular intervals. To initiate downloading of updates regardless of the download schedule, see Synchronize the vSphere Lifecycle Manager Depot .

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Configure**

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Settings** tab, select **Administration > Patch Setup**.

3 Click the **Change Download Source** button.

   The **Change Download Source Type** dialog box opens.

4 Select the **Download patches directly from the Internet** option and click **Save**.

Configure vSphere Lifecycle Manager to Use a Shared Repository as a Download Source

You can configure vSphere Lifecycle Manager to use a shared repository as a source for downloading ESXi images, vendor add-ons, and additional components.

You cannot use folders on a network drive as a shared repository. vSphere Lifecycle Manager does not download updates from folders on a network share in the Microsoft Windows Uniform Naming Convention form (such as `\\Computer_Name_or_Computer_IP\Shared`), or on a mapped network drive (for example, `Z:\`).

The downloading of updates takes place at configurable regular intervals. To initiate downloading of updates regardless of the download schedule, see Synchronize the vSphere Lifecycle Manager Depot .

Prerequisites

- Create a shared repository by using UMDS and host the repository on a Web server or a local disk. For detailed information about exporting the upgrades, update binaries, and update metadata in Export the Downloaded Data.
- Verify that UMDS is of version compatible with the version of vSphere Lifecycle Manager that you are using. For more information about compatibility, see Installing, Setting Up, and Using the Update Manager Download Service.
- Required privileges: **VMware vSphere Lifecycle Manager.Configure**.

Procedure

1. Navigate to the vSphere Lifecycle Manager home view.
   a. In the vSphere Client, select **Menu > Lifecycle Manager**.
   b. Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Administration > Patch Setup**.
3. Click the **Change Download Source** button.

   The **Change Download Source Type** dialog box opens.
4. Select the **Download patches from a UMDS shared repository** option and enter a path or URL address to the shared repository.

   For example, `C:\`*`repository_path`*`\`, `https://`*`repository_path`*`/` or `http://`*`repository_path`*`/`.

   In these examples, *repository_path* is the path to the folder with the exported downloaded upgrades, patches, extensions, and notifications. In an environment where vSphere Lifecycle Manager does not have direct access to the Internet, but is connected to a physical machine that has access to the Internet, the folder can be on a Web server.

   You can specify an HTTP or HTTPS address, or a location on the disk where vSphere Lifecycle Manager runs. HTTPS addresses are supported without any authentication.

5 Click **Save**.

vCenter Server validates the URL. You can use the path to the shared repository only when the validation is successful. If the validation fails, vSphere Lifecycle Manager reports a reason for the failure.

Important If the updates in the folder that you specify are downloaded with a UMDS version that is not compatible with the vCenter Server version that you use, the validation fails and you receive an error message.

Results

The shared repository is used as the main source for downloading software updates. Downloading from the repository is enabled by default.

Example: Using a Folder or a Web Server as a Shared Repository

You can use a folder or a Web server as a shared repository.

- When you use a folder as a shared repository, *repository_path* is the path to the top-level directory that stores the patches and notifications exported from UMDS.

  For example, use UMDS to export the patches and notifications to the `F:\` drive, which is a drive mapped to a plugged-in USB device on the physical machine where UMDS is installed. Then, plug in the USB device to the physical machine where vSphere Lifecycle Manager runs. The device is mapped as `E:\` and the folder to configure as a shared repository for vSphere Lifecycle Manager is `E:\`.

- When you use a Web server as a shared repository, *repository_path* is the path to the top-level directory on the Web server that stores the patches exported from UMDS.

  For example, export the patches and notifications from UMDS to `C:\docroot\exportdata`. If the folder is configured on a Web server and is accessible from other physical machines at the URL `https://`*`umds_host_name`*`/exportdata`, the URL to configure as a shared repository in vSphere Lifecycle Manager is `https://`*`umds_host_name`*`/exportdata`.

Run the VMware vSphere vSphere Lifecycle Manager Update Download Task

If you change the download source, you must run the VMware vSphere vSphere Lifecycle Manager Update Download task to download any new updates.

Procedure

1 In the vSphere Client, navigate to a vCenter Server instance.

2 On the **Configure** tab, select **Scheduled Tasks**.

3 In the **Scheduled Tasks** pane, select the **VMware vSphere Lifecycle Manager Update Download** task and click **Run**.

Results

You can see the running task listed in the **Recent Tasks** pane.

Add a New Download Source

You can add a new download source for vSphere Lifecycle Manager by providing a URL to the online depot or the UMDS repository that you want to use. Additionally, you can edit or delete a download source. You can also temporarily stop vSphere Lifecycle Manager from downloading updates from a particular download source.

Add a New Download Source

If you use the Internet as a download source for updates, you can add URL addresses to third-party online depots. vSphere Lifecycle Manager downloads software updates from all the online depots that you configured it to use. Update metadata are downloaded from the online depots to the local vSphere Lifecycle Manager depot.

The default download source for vSphere Lifecycle Manager is the official VMware depot.

Starting with vSphere 7.0, the official VMware online depot also hosts vendor add-ons and VMware-certified device drivers. Unlike previous releases, all software that you need to install, update, or customize the ESXi version of your hosts is available in the official VMware online depot.

Downloading updates takes place at configurable regular intervals. To initiate the downloading of updates regardless of the download schedule, see Synchronize the vSphere Lifecycle Manager Depot .

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Configure**

Procedure

1. Navigate to the vSphere Lifecycle Manager home view.

   a. In the vSphere Client, select **Menu > Lifecycle Manager**.

   b. Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2. On the **Settings** tab, select **Administration > Patch Setup**.

3. In the **Patches downloaded from the Internet** pane, click **New**.

   The **New Download Source** dialog box opens.

4 Enter a URL address to a new download source.

vSphere Lifecycle Manager supports both HTTP and HTTPS URL addresses. Use HTTPS URL addresses to download data securely. The URL addresses that you add must be complete and contain an `index.xml` file, which lists the vendor and the vendor index.

Note The proxy settings that vSphere Lifecycle Manager uses are also applicable to third-party URL addresses.

5 (Optional) Enter a short description for the download source.

6 Click **Save**.

Results

The new location is added to the list of download sources and downloading from it is enabled by default.

Modify a Download Source

You can edit or delete a download source from the list of vSphere Lifecycle Manager download sources. You can also allow or disallow vSphere Lifecycle Manager to download updates from a particular download source.

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Configure**

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Settings** tab, select **Administration > Patch Setup**.

3 In the **Patches downloaded from the Internet** pane, select a URL address from the list of download sources and select your task.

   - Click **Edit** to edit the source URL or the description for the selected download source.
   - Click **Enable** or **Disable** to allow or disallow downloading from the selected download source.

- Click **Delete** to delete the selected download source.

Note You cannot edit or delete the default VMware download source for ESXi updates. You can only allow or disallow vSphere Lifecycle Manager to use it for downloading update metadata from it.

Configure the vSphere Lifecycle Manager Automatic Download Task

Downloading host updates and related metadata is a predefined automatic process that you can modify. The automatic download task is enabled by default and starts immediately after you deploy vCenter Server. After the initial download, the task runs according to its schedule.

The default schedule settings ensure frequent checks, but you can change the schedule if your environment requires you to adjust the frequency of the checks.

If you need the latest software updates, you might want to reduce the time interval between the checks for updates. By contrast, if you are not concerned about the latest updates, if you want to reduce the network traffic, or if you cannot access the update servers, you might want to increase the time interval between the checks for updates.

The automatic download of update metadata is enabled by default and the default task name is VMware vSphere vSphere Lifecycle Manager Update Download. You can change the configuration of the task.

Prerequisites

- Verify that the machine on which vSphere Lifecycle Manager runs has access to the Internet.
- Required privileges: **VMware vSphere Lifecycle Manager.Configure**.

Procedure

1. Navigate to the vSphere Lifecycle Manager home view.
    a. In the vSphere Client, select **Menu > Lifecycle Manager**.
    b. Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

        The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.
2. On the **Settings** tab, select **Administration > Patch Downloads**.
3. In the **Automatic Download Settings** pane, click the **Edit** button.

    The **Edit Settings for Automatic Patch Downloads** dialog box opens.

4 Select the **Download patches** check box and configure the schedule and settings for the download.

   To receive notification emails after the download task finishes, you must configure mail settings for the vSphere Client. For more information, see the *vCenter Server and Host Management* documentation.

5 Click **Save** to save your changes and close the dialog box.

Results

The automatic download task runs according to the schedule you configured.

Installing, Setting Up, and Using the Update Manager Download Service

VMware vSphere Update Manager Download Service (UMDS) is an optional module of vSphere Lifecycle Manager. UMDS downloads software metadata, software binaries, and notifications that might not otherwise be available to vSphere Lifecycle Manager.

For security reasons and deployment restrictions, vSphere, including vSphere Lifecycle Manager, might be installed in a secured network that is disconnected from other local networks and the Internet. vSphere Lifecycle Manager requires access to patch information to function properly. If you are using such an environment, you can install UMDS on a computer that has Internet access. UMDS downloads upgrades, patch binaries, and patch metadata, and then you can export the downloads to a portable media drive so that they become accessible to vSphere Lifecycle Manager. If the server on which vCenter Server is installed has no Internet access, but is connected to a server that has Internet access, you can automate the export process and transfer files from UMDS to the vSphere Lifecycle Manager depot by using a Web server on the machine on which UMDS is installed.

UMDS is available for installation only on Linux-based operating systems. Installing UMDS on a Windows machine is no longer supported. Administrator access is not a requirement for downloading patches with UMDS that runs on Linux. The machine on which you install UMDS must have Internet access.

UMDS 8.0 supports patch recalls and notifications. A patch is recalled if the released patch has problems or potential issues. After you download patch data and notifications with UMDS, and export the downloads so that they become available to vSphere Lifecycle Manager, vSphere Lifecycle Manager deletes the recalled patches.

You can use UMDS to download updates that are packaged and distributed components, but it also works with legacy bulletins.

Compatibility Between UMDS and vSphere Lifecycle Manager

UMDS must be of the same version as vSphere Lifecycle Manager. For example, vSphere Lifecycle Manager 8.0 is compatible and can work only with UMDS 8.0. If you are using vSphere Lifecycle Manager of an Update release version, UMDS must be of the same Update release version.

Installing UMDS

In vSphere 8.0 release, the UMDS 8.0 is bundled with the vCenter Server appliance 8.0. You can use the UMDS bundle from the vCenter Server appliance to install UMDS 8.0 on a separate Linux-based system.

UMDS is a 64-bit application and requires a 64-bit Linux-based system.

Note You cannot upgrade UMDS that runs on a Linux-based operating system. You can uninstall the current version of UMDS, perform a fresh installation of UMDS according to all system requirements, and use the existing patch store from the UMDS that you uninstalled.

Supported Linux-Based Operating Systems for Installing UMDS

The Update Manager Download Service (UMDS) can run on a limited number of Linux-based operating systems.

- VMware Photon™ 5.0
- Ubuntu 14.0.4
- Ubuntu 18.04
- Ubuntu 18.04 LTS
- Ubuntu 20.04 LTS
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 8.1

  Note When you use Red Hat Enterprise Linux 8.1, you must install the `libnsl` package version 2.28 or later on the system where UMDS is deployed. If the package is not present on the system, UMDS operations might fail with the following error:

  ```
  Error while loading shared libraries: libnsl.so.1: cannot open shared object file: No such
  file or directory.
  ```

- Red Hat Enterprise Linux 8.3
- Red Hat Enterprise Linux 8.5

- Red Hat Enterprise Linux 8.6
- Red Hat Enterprise Linux 8.10
- Red Hat Enterprise Linux 9.0
- Red Hat Enterprise Linux 9.2

Install UMDS on a Linux OS

If the vCenter Server appliance 8.0 where vSphere Lifecycle Manager runs does not have access to the Internet, you can install UMDS on a Linux-based operating system to download update binaries and metadata.

Prerequisites

- Verify you have administrative privileges on the Linux machine where you install the UMDS.
- Mount the ISO file of the vCenter Server appliance 8.0 to the Linux machine.

Procedure

1 In the Linux machine, open the Command Shell.

2 From the vCenter Server ISO that you mounted to the Linux machine, copy the `VMware-UMDS-8.0.1-`*`build_number`*`.tar.gz` file to the Linux machine.

3 Unarchive the `VMware-UMDS-8.0.1-`*`build_number`*`.tar.gz` file by running `tar -xvzf VMware-UMDS-8.0.1-`*`build_number`*`.tar.gz` and navigate to the newly extracted directory `/vmware-umds-distrib`.

   For example, if you unarchived the `VMware-UMDS-8.0.1-`*`build_number`*`.tar.gz` file, to a directory you created with the name *umds*, your navigation path is `/`*`umds`*`/vmware-umds-distrib`.

4 Run the file UMDS installation script.

   The script has the following file name: `vmware-install.pl`.

5 Read and accept the EULA.

6 Select a directory where to install the UMDS.

   The default UMDS installation location is `usr/local/vmware-umds`.

7 Enter the UMDS proxy settings.

   You can also change proxy configuration after you install UMDS by using the following command:

```
vmware-umds -S --proxy <proxyAddress:port>
```

8 Select a directory where to store the patches.

Important The patch store directory must be different from the UMDS installation directory. The default patch store location is `/var/lib/vmware-umds`.

Results

UMDS is installed.

Uninstall UMDS from a Linux OS

To use the latest UMDS version on your Linux-based system, you must first uninstall the current version of UMDS. No direct upgrade path is available to a later version of UMDS.

Prerequisites

- Verify you have administrative privileges on the Linux machine where UMDS runs.

Procedure

1 In the Linux machine, open the Command Shell.

2 Navigate to the UMDS installation directory, and locate the file `vmware-uninstall-umds.pl`.

The default UMDS installation location is `usr/local/vmware-umds`.

3 Run the `./vmware-uninstall-umds.pl` command.

4 To confirm that you want to uninstall UMDS from the system, enter **Yes**.

The UMDS uninstallation procedure starts.

5 (Optional) Remove PostgreSQL Database from you Linux machine.

For information about uninstalling PostgreSQL Database, go to the official PostgreSQL documentation.

Results

UMDS is uninstalled from the Linux system.

What to do next

You can upgrade your Linux OS, and install a later compatible version of UMDS.

Setting Up UMDS

You can set up UMDS to download patches for ESXi hosts. You can also set up UMDS to download ESXi 6.7, ESXi 7.0, and ESXi 8.0 patch binaries, patch metadata, and notifications from third-party portals.

Administrator access is not a requirement for downloading patches if UMDS runs on Linux.

You can set up UMDS to download ESXi 6.7, ESXi 7.0, and ESXi 8.0 patches from the official VMware depot and third-party portals.

The best practice is to use a job scheduler, for example cron job, to create a job that periodically triggers UMDS to download the upgrades, patches, and notifications.

Set Up the Data to Download with UMDS

By default, UMDS downloads patch binaries, patch metadata, and notifications for hosts. You can specify which patch binaries and patch metadata to download with UMDS.

Procedure

1 Log in to the machine where UMDS is installed, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Specify the updates to download.

   - To set up a download of all ESXi host updates, run the following command:

     ```
     vmware-umds -S --enable-host
     ```

   - To deactivate the download of host updates, run the following command:

     ```
     vmware-umds -S --disable-host
     ```

What to do next

Download the selected data.

Change the UMDS Patch Repository Location

UMDS downloads upgrades, patch binaries, patch metadata, and notifications to a folder that you can specify during the UMDS installation.

The default folder to which UMDS downloads patch binaries and patch metadata on a Linux machine is `/var/lib/vmware-umds` .

You can change the folder in which UMDS downloads data after you install UMDS.

If you have already downloaded host updates, copy all the files and folders from the old location to the new patch store location. The folder in which UMDS downloads patch binaries and patch metadata must be located on the machine on which UMDS is installed.

Procedure

1 Log in as an administrator to the machine where UMDS is installed, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Change the patch repository directory by running the command:

```
vmware-umds -S --patch-store your_new_patchstore_folder
```

In this example, *your_new_patchstore_folder* is the path to the new folder in which you want to download the patch binaries and patch metadata.

Results

You successfully changed the directory in which UMDS stores patch data.

What to do next

Download data using UMDS.

Configure URL Addresses for Hosts

You can configure UMDS to connect to the websites of third-party vendors to download ESXi 6.7, ESXi 7.0, and ESXi 8.0 host patches and notifications.

Procedure

1 Log in to the machine where UMDS runs, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Configure UMDS to download data from the new URL address.

   - To add a new URL address for downloading patches and notifications for ESXi 6.7, ESXi 7.0, or ESXi 8.0 hosts, run the following command:

     ```
     vmware-umds -S --add-url https://host_URL/index.xml --url-type HOST
     ```

4 (Optional) Remove a URL address, so that UMDS does not download data from it anymore.

   Downloaded data is retained and can be exported. Use the following command:

   ```
   vmware-umds -S --remove-url https://URL_to_remove/index.xml
   ```

Results

You configured UMDS to download host patches and notifications from specific URL addresses.

What to do next

Download the patches and notifications by using UMDS.

Using UMDS

You use UMDS in air-gap scenarios, where vSphere Lifecycle Manager has no access to the Internet. You first use UMDS to download software and notifications and then you export the data, so that it becomes available to vSphere Lifecycle Manager.

To use UMDS, the machine on which you install it must have Internet access. After you download the upgrades, patch binaries, patch metadata, you can export the data to a Web server or a portable media drive, such as CD or USB flash drive. Then, you must set up vSphere Lifecycle Manager to use the folder on the Web server or the media drive (mounted as a local disk) as a download source.

Download the Specified Data Using UMDS

After you set up UMDS, you can download upgrades, patches and notifications to the machine on which UMDS is installed.

Administrator level access is not a requirement for downloading data with UMDS that runs on Linux.

Procedure

1 Log in to the machine where UMDS is installed, and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Download the selected updates.

   ```
   vmware-umds -D
   ```

   This command downloads all the upgrades, patches and notifications from the configured sources for the first time. Subsequently, it downloads all new patches and notifications released after the previous UMDS download.

4 (Optional) If you have already downloaded upgrades, patches, and notifications and want to download them again, you can include the start and end times to restrict the data to download.

   The command to re-download patches and notifications deletes the existing data from the patch store (if present) and re-downloads it.

   To re-download the upgrades, patches and notifications that were downloaded in November 2010, for example, run the following command:

   ```
   vmware-umds -R --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59
   ```

   The data previously downloaded for the specified period is deleted and downloaded again.

What to do next

Export the downloaded upgrades, patches, and notifications.

Export the Downloaded Data

You can export downloaded upgrades, patches, and notifications to a specific location that serves as a shared repository for vSphere Lifecycle Manager. You can configure vSphere Lifecycle Manager to use the shared repository as a patch download source. The shared repository can also be hosted on a Web server.

Administrator level access is not a requirement for exporting the downloaded data with UMDS that runs on Linux.

Prerequisites

If you installed UMDS with an existing download directory, verify that you perform at least one download by using UMDS 8.0 before you export updates.

Procedure

1 Log in to the machine where UMDS is installed and open a **Command Prompt** window.

2 Navigate to the directory where UMDS is installed.

   The default location in 64-bit Linux is `/usr/local/vmware-umds`.

3 Specify the export parameters and export the data.

   ```
   vmware-umds -E --export-store repository_path
   ```

   In the command, you must specify the full path of the export directory.

   If you are working in a deployment in which the vCenter Server is installed on a machine connected to the machine on which UMDS is installed, *repository_path* can be the path to the folder on the Web server that serves as a shared repository.

   If the vCenter Server is installed on a machine in an isolated and secure environment, *repository_path* can be the path to a portable media drive. Export the downloads to the portable media drive to physically transfer the patches to the machine on which vCenter Server is installed and vSphere Lifecycle Manager runs.

   The data you downloaded by using UMDS is exported to the path you specify. Make sure that all files are exported. You can periodically export from UMDS and populate the shared repository so that vSphere Lifecycle Manager can use the new patch binaries and patch metadata.

4 (Optional) You can export the ESXi patches that you downloaded during a specified time window.

   For example, to export the patches downloaded in November 2010, run the following command:

   ```
   vmware-umds -E --export-store repository-path --start-time 2010-11-01T00:00:00 --end-time 2010-11-30T23:59:59
   ```

What to do next

Configure vSphere Lifecycle Manager to use a shared repository as a patch download source. For more information, see Configure vSphere Lifecycle Manager to Use a Shared Repository as a Download Source.

vSphere Lifecycle Manager Remediation Settings

3

Whether you manage the ESXi hosts in your environment with baselines or with images, you can configure the behavior of vSphere Lifecycle Manager during remediation.

The vSphere Lifecycle Manager remediation settings for hosts and clusters that use baselines differ from the remediation settings for hosts and clusters that you manage with a single vSphere Lifecycle Manager image. For example, allowing the installation of software on PXE booted hosts and the removal of media devices before maintenance mode are settings that you can configure only for hosts and clusters that use baselines. Virtual machine migration settings, maintenance mode settings, and Quick Boot are examples of remediation settings that you can configure for both hosts and clusters that use baselines or images.

You can modify the default vSphere Lifecycle Manager settings only if you have the appropriate privileges. The permission must be assigned to the vCenter Server instance where vSphere Lifecycle Manager runs. For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation. For a list of the vSphere Lifecycle Manager privileges and their descriptions, see Required Privileges for Using vSphere Lifecycle Manager and vSphere Configuration Profiles.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can configure the remediation settings for each vSphere Lifecycle Manager instance. The configuration properties that you modify are applied only to the vSphere Lifecycle Manager instance that you specify, and are not propagated to the other instances in the domain.

How Do Cluster Settings Affect Remediation?

When you remediate ESXi hosts that are in a cluster, certain cluster settings might cause remediation failure. You must configure the cluster settings in such a way as to ensure successful remediation.

Distributed Resource Scheduler (DRS)

Updates might require a host to enter maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure availability, you can activate DRS for the cluster and you can configure it for vSphere vMotion. In this case, before the host is put in maintenance mode, vCenter Server migrates the virtual machines to another ESXi host within the cluster.

To help ensure vSphere vMotion compatibility between the hosts in the cluster, you can enable Enhanced vMotion Compatibility (EVC). EVC ensures that all hosts in the cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. EVC prevents migration failures due to incompatible CPUs. You can enable EVC only in a cluster where the host CPUs meet the compatibility requirements. For more information about EVC and the requirements that the hosts in an EVC cluster must meet, see the *vCenter Server and Host Management* documentation.

Distributed Power Management (DPM)

If a host has no running virtual machines, DPM might put the host in standby mode, which might interrupt a vSphere Lifecycle Manager operation. So, to make sure that all vSphere Lifecycle Manager operations finish successfully, you must deactivate DPM during these operations.

For successful remediation, you must configure vSphere Lifecycle Manager to deactivate DPM. After the remediation task finishes, vSphere Lifecycle Manager restores DPM. If DPM has already put a host in standby mode, vSphere Lifecycle Manager powers on the host before compliance checks, remediation, and staging. After the respective task finishes, vSphere Lifecycle Manager turns on DPM and lets DPM put the host into standby mode, if needed. vSphere Lifecycle Manager does not remediate powered off hosts.

If a host is put in standby mode and DPM is manually deactivated for a reason, vSphere Lifecycle Manager does not remediate or power on the host.

HA Admission Control

Within a cluster, you must deactivate HA admission control temporarily to let vSphere vMotion proceed. This action prevents downtime for the machines on the hosts that you remediate. You can configure vSphere Lifecycle Manager to deactivate HA admission control during remediation. After the remediation of the entire cluster is complete, vSphere Lifecycle Manager restores the HA admission control settings. vSphere Lifecycle Manager deactivates HA admission control before remediation, but not before compliance checks. Additionally, for clusters that you manage with baselines, vSphere Lifecycle Manager deactivates HA admission control before staging.

Note

Deactivating HA admission control before you remediate a two-node cluster that uses a single vSphere Lifecycle Manager image causes the cluster to practically lose all its high availability guarantees. The reason is that when one of the two hosts enters maintenance mode, vCenter Server cannot failover virtual machines to that host and HA failovers are never successful. For more information about HA admission control, see the *vSphere Availability* documentation.

Fault Tolerance (FT)

If FT is turned on for any of the virtual machines on a host within a cluster, you must temporarily turn off FT before performing any vSphere Lifecycle Manager operation on the cluster. If FT is turned on for any of the virtual machines on a host, vSphere Lifecycle Manager does not remediate that host. You must remediate all hosts in a cluster with the same updates, so that FT can be reactivated after remediation. A primary virtual machine and a secondary virtual machine cannot reside on hosts of different ESXi versions and patch levels.

Read the following topics next:

- Configuring vSphere Lifecycle Manager for Fast Upgrades
- Configuring vSphere Lifecycle Manager for Live Patches
- How to Configure the vSphere Lifecycle Manager Remediation Settings

Configuring vSphere Lifecycle Manager for Fast Upgrades

During cluster or host remediation, you can preserve the state of the virtual machines in the host memory and restore them from memory after the remediation finishes. Suspending virtual machines to memory and using the Quick Boot functionality significantly reduces the time for remediation, minimizes system boot time, and reduces the downtime of system and services.

During remediation with vSphere Lifecycle Manager, migrating virtual machines from the host that is under remediation to another host takes a considerable amount of time. After remediation, vSphere Lifecycle Manager migrates back the virtual machines to the remediated host. However, you can configure vSphere Lifecycle Manager to suspend virtual machines to memory instead of migrating them, powering them off, or suspending them to disk.

You can use the suspend to memory functionality only for patching operations, for example, when you remediate a cluster or a standalone host to apply to it a hot patch, express patch, and so on. You cannot use the suspend to memory option for upgrade operations, for example when you upgrade your ESXi hosts from version 7.0 to version 8.0.

Suspend Virtual Machines to Memory

Suspend to memory is an option that you can use only for clusters or hosts that you manage with vSphere Lifecycle Manager images. The functionality works together with the Quick Boot setting to optimize the remediation process and minimize virtual machine downtime.

You enable vSphere Lifecycle Manager to suspend virtual machines to memory when you configure the vSphere Lifecycle Manager host remediation settings. During remediation pre-check and remediation, vSphere Lifecycle Manager verifies that the suspend to memory option is indeed applicable to the host or cluster under remediation. If for some reason suspend to memory is inapplicable, vSphere Lifecycle Manager reports an error and prevents remediation from proceeding.

During a suspend to memory operation, virtual machines remain in a suspended state for some time. So, suspending virtual machines to memory might impact the workloads running on those virtual machines. The impact is similar to the impact that the suspend to disk operation might have on virtual machines and workloads.

Caution As a best practice, always take snapshots of the virtual machines with critical workloads before you start remediation when the suspend to memory option is activated.

vSphere Lifecycle Manager might not suspend to memory all virtual machines on the host even if you activated the feature for the entire cluster or the standalone host. In some cases, vSphere Lifecycle Manager is still able to proceed with the remediation of the host, even if some virtual machines cannot be suspended to memory.

- vSphere ESX Agent Manager (EAM) virtual machines

  vSphere Lifecycle Manager powers off the EAM virtual machines after all other virtual machines are suspended. Similarly, vSphere Lifecycle Manager powers on the EAM virtual machines before any other virtual machines are resumed from memory. None of the suspended virtual machines is resumed until the EAM virtual machines are powered on.

- vSphere Cluster Services virtual machines

  vSphere Lifecycle Manager first migrates to another host the vSphere Cluster Services virtual machines, and then suspends to memory the rest of the virtual machines on the host.

Similarly, vSphere Lifecycle Manager does not suspend to memory the management virtual appliances for some VMware products and solutions. However, if a virtual machine for any of the following products or solutions runs on a host, the suspend to memory pre-check fails and vSphere Lifecycle Manager does not proceed with the remediation of the respective host:

- vCenter Server
- vSAN witness virtual machine
- vSphere IaaS control plane
- NSX
- VMware HCX
- vSphere Replication
- Site Recovery Manager
- VMware Aria products

Note Third-party virtual machines do get suspended during remediation, if the Suspend to memory option is activated.

Quick Boot

Quick Boot is a setting that you can use with clusters or standalone hosts that you manage with vSphere Lifecycle Manager images and vSphere Lifecycle Manager baselines. Using Quick Boot optimizes the host patching and upgrade operations. Quick Boot lets vSphere Lifecycle Manager reduce the remediation time for hosts that undergo patch and upgrade operations. Patch and upgrade operations do not affect the hardware of a host. If the Quick Boot feature is activated, vSphere Lifecycle Manager skips the hardware reboot (the BIOS or UEFI firmware reboot). As a result, the time an ESXi host spends in maintenance mode is reduced and the risk of failures during remediation is minimized.

To configure vSphere Lifecycle Manager to suspend virtual machines to the host memory, you must activate Quick Boot. However, you can activate Quick Boot even if you decide not to use the Suspend to memory option.

Requirements for Using Suspend to Memory

Several factors might hinder the applicability of the suspended to memory option. If for some reason suspend to memory is inapplicable, vSphere Lifecycle Manager reports an error and prevents remediation from proceeding. Suspend to memory works under the following conditions:

- The host supports the suspend to memory functionality.
- Quick Boot is activated for the cluster or the standalone host and the host under remediation supports Quick Boot.
- The remediation does not involve host upgrades or firmware upgrade.
- The host and the virtual machines meet certain requirements.

Host Requirements	**Virtual Machine Requirements**
■ The host has enough free memory. ■ The host has sufficient free low memory. ■ The host has enough free memory per NUMA node to start after a reboot. ■ The host has enough reservation available ■ The host does not use swapped or compressed pages of virtual machines.	■ The virtual machines do not have any passthrough devices. ■ The virtual machines do not have latency sensitivity set to high. ■ The virtual machines are not fault tolerant. ■ The virtual machines are not encrypted. ■ The virtual machines do not use persistent memory. ■ The virtual machines do not have virtual SGX or SEV devices. ■ The virtual machines do not have the suspend feature deactivated. ■ The virtual machines are not frozen source virtual machines during an Instant Clone operation.

Suspend to Memory and vSphere High Availability (HA)

When you configure vSphere Lifecycle Manager to suspend virtual machines to memory during remediation, vSphere HA provides protection for the suspended virtual machines in cases of failure at the virtual machine or host level. By modifying the vSphere HA advanced options, you can set a timeout value for suspended to memory virtual machines. If a suspended to memory virtual machine is not responsive for the specified time, vSphere HA powers on the virtual machine on the original host or on another host.

- If you deactivate or reconfigure vSphere HA for the cluster during remediation, vSphere HA can no longer protect the suspended virtual machines. Before you change the vSphere HA configuration, make sure that no hosts in the cluster are in maintenance mode and the suspended virtual machines are powered on.
- If you modify the `das.failoverDelayForSuspendToMemoryVmsSecs` advanced option for vSphere HA after you configure vSphere Lifecycle Manager to use the suspend to memory option, the newly specified timeout value might not apply to the virtual machines. If you need to modify the default value of the `das.failoverDelayForSuspendToMemoryVmsSecs` option, ensure that you modify it before you start remediation to ensure that the new value is in effect.
- If the suspend to memory operation fails, vSphere HA determines the most appropriate failover host after the specified timeout value expires. The failover host might be the original host or another one.
- You must synchronize the server time for all ESXi hosts in the cluster. If the hosts are not synchronized, vSphere HA might not respect the specified timeout period and initiate failover earlier or later.

For more information about using and configuring vSphere HA, see the *vSphere Availability* documentation.

Configuring vSphere Lifecycle Manager for Live Patches

When you enable the Live Patch setting, you can apply security patches and urgent bug fixes to all hosts in a cluster that you manage with a vSphere Lifecycle Manager image with minimal disruption to your workloads.

Starting with vSphere 8.0 Update 3, you can use the Live Patch setting to deploy patches with resolved security and functional issues to all ESXi hosts in a cluster managed with a single image. During remediation, vSphere Lifecycle Manager does not place the hosts in the cluster into maintenance mode, hosts are not rebooted and there is no need to migrate the virtual machines running on the hosts in the cluster.

To configure vSphere Lifecycle Manager to perform live patch operations on the hosts in a cluster managed with an image, you must activate Live Patch. See Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image .

Requirements for Using Live Patch

You use vSphere Lifecycle Manager to install live patches on hosts that are part of a cluster managed with a single image, only in case the following conditions are met:

- vCenter Server must be of version 8.0 Update 3 and later.
- All ESXi hosts in the cluster managed with a vSphere Lifecycle Manager image must be of version 8.0 Update 3 and later.
- You use the Live Patch functionality only to upgrade hosts in a cluster that you manage with a vSphere Lifecycle Manager image.
- All hosts in the cluster managed with a single image must support the Live Patch functionality. If you activate Live Patch for a vCenter Server instance or a cluster and you try to install a live patch on the cluster with hosts that require maintenance mode, remediation is blocked. You can view details about the compliance of the cluster against the selected live patch image for further information.
- vSphere Lifecycle Manager can install a live patch only to a host that is eligible to be updated with a specific live patch release of the VMware base image. vSphere Lifecycle Manager image depot provides information about all the possible versions of the ESXi host image which you can update with a specific Live Patch release. For more information about how to browse the depot, see Browsing the vSphere Lifecycle Manager Depot.
- vSphere DRS must be enabled on the cluster managed with a single image before you try to install a live patch on all hosts.
- You must deactivate the parallel remediation setting before you try to install a live patch on the hosts in the cluster. If you have both settings enabled, the remediation pre-check reports this as an issue for a successful remediation and provides you with possible solutions. Live patches can only be installed on the hosts in a cluster managed with a single image in sequence.

How to Configure the vSphere Lifecycle Manager Remediation Settings

In the vSphere Client, you configure separately the vSphere Lifecycle Manager remediation settings for the hosts and clusters that you manage with a single image and with baselines.

The global remediation settings are valid for all hosts and clusters that you manage with images or baselines respectively. For clusters or standalone hosts that you manage with a single image, you can override the global remediation settings and use specific remediation settings for a particular cluster or host.

Hosts that are in a vSAN cluster can enter maintenance mode only one at a time. This behavior is a peculiarity of the vSAN cluster. For more information about the vSphere Lifecycle Manager behavior during the remediation of hosts in a vSAN cluster, see Remediation Specifics of vSAN Clusters .

Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image

You can configure how ESXi hosts and VMs behave before and during the remediation of a cluster or a standalone host that you manage with a single image.

For information about automatically triggered hardware compatibility checks, which is a functionality that is also applicable only to vSAN clusters, see When Does the Hardware Compatibility Check Task Run.

Prerequisites

- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.
- To use Quick Boot, verify that the ESXi host is compatible with the feature. For more information, see Quick Boot.

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Settings** tab, select **Cluster lifecycle > Images**.

3 Edit the cluster or standalone host remediation settings.

   - In the **Images** pane, click the **Edit** button.

     The **Edit Cluster Remediation Settings** dialog box opens.

   - In the **Standalone Host Images** pane, click the **Edit** button.

     The **Edit Standalone Host Remediation Settings** dialog box opens.

4 Configure the remediation settings for clusters and standalone hosts that use images, and click **Save**.

Setting	Description
Quick Boot	Quick Boot reduces the host reboot time during remediation. By default, Quick Boot is turned on. You can configure this setting for a cluster or a standalone host.
Live Patch	Live Patch allows you to perform low-disruption upgrades of the ESXi hosts in a cluster managed with an image. When you turn on Live Patch, you can install the latest security patches and bug fixes without placing the hosts into maintenance mode or evacuating virtual machines from the hosts. See Configuring vSphere Lifecycle Manager for Live Patches. By default, Live Patch is turned off. You can configure this setting only for a cluster that you manage with a single image.
VM power state	The **VM power state**option lets you control the behavior of the virtual machines that run on the ESXi host. You can select from the following options. ■ **Do not change power state** ■ **Suspend to disk** ■ **Suspend to memory** To select the **Suspend to memory** option, you must turn on Quick Boot. Otherwise, the **Suspend to memory** option is dimmed. Together with Quick Boot, the **Suspend to memory** option provides faster host upgrades. vSphere Lifecycle Managersuspends to the host memory and not to the disk the powered on virtual machines on the host. After the Quick Boot, the suspended virtual machines are resumed from memory. ■ **Power off** The default selection is **Do not change power state**. You can configure these options for a cluster or a standalone host.
VM migration	You can configure vSphere Lifecycle Manager to migrate the suspended and powered off virtual machines from the hosts that must enter maintenance mode to other hosts in the cluster. By default, the **Migrate powered off and suspended VMs to other hosts in the cluster** check box is selected. If you have virtual machines with passthrough devices on a host in a DRS cluster, make sure that you automate the migration of such virtual machines. For more information, see the VMware knowledge base article at https://kb.vmware.com/s/article/88271. You can configure this setting only for a cluster that you manage with a single image.
Retry policy	You can configure how vSphere Lifecycle Manager behaves if a host fails to enter maintenance mode or if staging or remediation for that host fails. You can configure vSphere Lifecycle Manager to wait for a specified retry delay period and to retry to put the host into maintenance mode as many times as you indicate in the **Number of retries** text box. You can configure this setting for a cluster or a standalone host.

Setting	Description
HA admission control	Admission control is a policy that vSphere HA uses to ensure failover capacity within a cluster. If vSphere HA admission control is enabled during remediation, vMotion might be unable to migrate the virtual machines within the cluster. Deactivating admission control allows a virtual machine to be powered on even if it causes insufficient failover capacity. When this happens, no warnings are presented, and the cluster does not turn red. If a cluster has insufficient failover capacity, vSphere HA can still perform failovers, and uses the VM Restart Priority setting to determine which virtual machines to power on first. **Note** Deactivating HA admission control before you remediate a two-node cluster causes the cluster to practically lose all its high availability guarantees. ■ If you select the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables HA admission control after remediation is complete. ■ If you deselect the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager skips remediating the clusters on which HA admission control is enabled. By default, the **Disable HA admission control on the cluster** check box is deselected. You can configure this setting only for a cluster that you manage with a single image.
DPM	VMware Distributed Power Management (DPM) monitors the resources consumed by the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state. ■ If you select the **Disable DPM on the cluster** option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables DPM after remediation is complete. ■ If you deselect the **Disable DPM on the cluster** option, vSphere Lifecycle Manager skips remediating the clusters on which DPM is enabled. By default, the **Disable DPM on the cluster** check box is selected. You can configure this setting only for a cluster that you manage with a single image.

Setting	Description
Hardware compatibility issues	vSphere Lifecycle Manager performs a hardware compatibility check as part of the remediation pre-check and the remediation tasks for vSAN clusters. You can configure vSphere Lifecycle Manager to prevent remediation when hardware compatibility issues exist for the cluster. ■ If you select the **Prevent remediation if hardware compatibility issues are found** option, vSphere Lifecycle Manager reports hardware compatibility issues as an error, which prevents remediation. ■ If you deselect the **Prevent remediation if hardware compatibility issues are found** option, vSphere Lifecycle Manager reports hardware compatibility issues as a warning, which does not prevent remediation. If the cluster is not vSAN-enabled, vSphere Lifecycle Manager does not perform a hardware compatibility check as part of the remediation pre-check or the remediation tasks. You can configure this setting only for a cluster that you manage with a single image.
Parallel remediation	Enabling parallel remediation allows you to remediate multiple ESXi hosts simultaneously. By selecting the **Parallel remediation** check box, you enable vSphere Lifecycle Manager to remediate all hosts that are in maintenance mode in parallel instead of in sequence. You can also specify the maximum number of concurrent remediations manually. **Note** If the hosts have NSX virtual distributed switches that are ready to be migrated to vSphere Distributed Switches, you must manually set the maximum number of parallel remediations to no more than 4. In cases when host switch migration is needed, if more than 4 hosts are remediated in parallel, the remediation might fail, because the host switch migration takes more time than the time vSphere Lifecycle Manager needs to complete the parallel remediation. You can configure this setting only for a cluster that you manage with a single image.

Results

These settings become the default remediation settings for clusters or standalone hosts that you manage with vSphere Lifecycle Manager images. For any cluster or host, you can change the default settings when you configure individual remediation tasks.

Override the Global vSphere Lifecycle Manager Remediation Settings for a Cluster or Host That You Manage with a Single Image

You can customize the remediation settings for a particular cluster or a standalone host while the global remediation settings remain intact and applicable to all other clusters or hosts that you manage with vSphere Lifecycle Manager images and that are in the same vCenter Server instance.

When you override the global remediation settings for a single cluster or host, the overrides are used during the remediation of that specific cluster or host. For all other clusters or hosts, the global remediation settings apply.

Prerequisites

- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.
- To enable Quick Boot, verify that the ESXi host is compatible with the feature. For more information, see Quick Boot.

Procedure

1. In the vSphere Client, navigate to a cluster or host that you manage with a single image.
2. On the **Updates** tab, select **Hosts > Image**.
3. In the **Image Compliance** card, click the horizontal ellipsis icon and select **Edit remediation settings**.
4. In the **Edit Remediation Settings** dialog box, configure the remediation settings of the target cluster or host and click **Save**.

Setting	Description
Quick Boot	Quick Boot reduces the host reboot time during remediation. By default, Quick Boot is enabled. You can configure this setting for a cluster or a standalone host.
Live Patch	Live Patch allows you to perform low-disruption upgrades of the ESXi hosts in a cluster managed with an image. When you turn on Live Patch, you can install the latest security patches and bug fixes without placing the hosts into maintenance mode or evacuating virtual machines from the hosts. See Configuring vSphere Lifecycle Manager for Live Patches. By default, Live Patch is turned off. You can configure this setting only for a cluster that you manage with a single image.
VM power state	The **VM power state**option lets you control the behavior of the virtual machines that run on the ESXi host. You can select from the following options. ■ **Do not change power state** ■ **Suspend to disk** ■ **Suspend to memory** To select the **Suspend to memory** option, you must enable Quick Boot. Otherwise, the **Suspend to memory** option is dimmed. Together with Quick Boot, the **Suspend to memory** option provides faster host upgrades. vSphere Lifecycle Manager suspends to the host memory and not to the disk the powered on virtual machines on the host. After the Quick Boot, the suspended virtual machines are resumed from memory. ■ **Power off** The default selection is **Do not change power state**. You can configure these options for a cluster or a standalone host.

Setting	Description
VM migration	You can configure vSphere Lifecycle Manager to migrate the suspended and powered off virtual machines from the hosts that must enter maintenance mode to other hosts in the cluster. By default, the **Migrate powered off and suspended VMs to other hosts in the cluster** check box is selected. If you have virtual machines with passthrough devices on a host in a DRS cluster, make sure that you automate the migration of such virtual machines. For more information, see the VMware knowledge base article at https://kb.vmware.com/s/article/88271. You can configure this setting only for a cluster that you manage with a single image.
Retry policy	You can configure how vSphere Lifecycle Manager behaves if staging or remediation fails, or if a host fails to enter maintenance mode. You can configure vSphere Lifecycle Manager to wait for a specified retry delay period and to retry to put the host into maintenance mode as many times as you indicate in the **Number of retries** text box. You can configure this setting for a cluster or a standalone host.
HA admission control	Admission control is a policy that vSphere HA uses to ensure failover capacity within a cluster. If vSphere HA admission control is enabled during remediation, vMotion might be unable to migrate the virtual machines within the cluster. Deactivating admission control allows a virtual machine to be powered on even if it causes insufficient failover capacity. When this happens, no warnings are presented, and the cluster does not turn red. If a cluster has insufficient failover capacity, vSphere HA can still perform failovers, and uses the VM Restart Priority setting to determine which virtual machines to power on first. **Note** Deactivating HA admission control before you remediate a two-node cluster causes the cluster to practically lose all its high availability guarantees. ■ If you select the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables HA admission control after remediation is complete. ■ If you deselect the **Disable HA admission control on the cluster** option, vSphere Lifecycle Manager skips remediating the clusters on which HA admission control is enabled. By default, the **Disable HA admission control on the cluster** check box is deselected. You can configure this setting only for a cluster that you manage with a single image.

<table>
<tr><th>Setting</th><th>Description</th></tr>
<tr><td>DPM</td><td>VMware Distributed Power Management (DPM) monitors the resources consumed by the running virtual machines in the cluster. If sufficient excess capacity exists, VMware DPM recommends moving virtual machines to other hosts in the cluster and placing the original host into standby mode to conserve power. If the capacity is insufficient, VMware DPM might recommend returning standby hosts to a powered-on state.
If you select the Disable DPM on the cluster option, vSphere Lifecycle Manager remediates the hosts in the cluster and re-enables DPM after remediation is complete.
If you deselect the Disable DPM on the cluster option, vSphere Lifecycle Manager skips remediating the clusters on which DPM is enabled.
By default, the Disable DPM on the cluster check box is selected.
You can configure this setting only for a cluster that you manage with a single image.</td></tr>
<tr><td>Hardware compatibility issues</td><td>vSphere Lifecycle Manager performs a hardware compatibility check as part of the remediation pre-check and the remediation tasks for vSAN clusters. You can configure vSphere Lifecycle Manager to prevent remediation when hardware compatibility issues exist for the cluster.
If you select the Prevent remediation if hardware compatibility issues are found option, vSphere Lifecycle Manager reports hardware compatibility issues as an error, which prevents remediation.
If you deselect the Prevent remediation if hardware compatibility issues are found option, vSphere Lifecycle Manager reports hardware compatibility issues as a warning, which does not prevent remediation.
If the cluster is not vSAN-enabled, vSphere Lifecycle Manager does not perform a hardware compatibility check as part of the remediation pre-check or the remediation tasks.
You can configure this setting only for a cluster that you manage with a single image.</td></tr>
<tr><td>Parallel remediation</td><td>Enabling parallel remediation allows you to remediate multiple ESXi hosts simultaneously. By selecting the Parallel remediation check box, you enable vSphere Lifecycle Manager to remediate all hosts that are in maintenance mode in parallel instead of in sequence. You can also specify the maximum number of concurrent remediations manually.
Note If the hosts have NSX virtual distributed switches that are ready to be migrated to vSphere Distributed Switches, you must manually set the maximum number of parallel remediations to no more than 4. In cases when host switch migration is needed, if more than 4 hosts are remediated in parallel, the remediation might fail, because the host switch migration takes more time than the time vSphere Lifecycle Manager needs to complete the parallel remediation.
You can configure this setting only for a cluster that you manage with a single image.</td></tr>
</table>

Results

These settings become the remediation settings for the selected cluster. vSphere Lifecycle Manager uses those settings for that cluster for all future remediation tasks. The global remediation settings remain unchanged and are applied to all other clusters.

In the **Image Compliance** card, vSphere Lifecycle Manager displays a message that the global remediation settings are overridden. Also, an option to reset the values appears in the card.

Configure the vSphere Lifecycle Manager Remediation Settings for Hosts and Clusters That You Manage with Baselines

You can configure how vSphere Lifecycle Manager behaves before and during remediation against a baseline or a baseline group. The remediation settings help ensure that vSphere Lifecycle Manager puts ESXi hosts in maintenance mode before remediation.

When you use vSphere Lifecycle Manager baselines, you can configure vSphere Lifecycle Manager to let other software initiate the remediation of PXE booted ESXi hosts. The remediation installs software modules on the hosts, but typically those host updates are lost after a reboot. To retain updates on stateless hosts after a reboot, use a PXE boot image that contains the updates. You can update the PXE boot image before applying the updates with vSphere Lifecycle Manager, so that the updates are not lost because of a reboot. vSphere Lifecycle Manager itself does not reboot the hosts, because it does not install updates requiring a reboot on PXE booted ESXi hosts.

Prerequisites

- Required privileges: **VMware vSphere Lifecycle Manager.Configure**
- To enable Quick Boot, verify that the ESXi host is compatible with the feature. For more information, see Quick Boot.

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Settings** tab, select **Cluster Lifecycle > Baselines**.

3 Click the **Edit** button.

   The **Edit Settings for Host Remediation** dialog box opens.

4 Configure the baselines remediation settings and click **Save**.

Option	Description
VM power State	You can configure vSphere Lifecycle Manager to power off or suspend all running virtual machines before host remediation. Alternatively, you can configure vSphere Lifecycle Manager not to change the power state of the virtual machines.
Maintenance mode failures	You can configure how vSphere Lifecycle Manager behaves if a host fails to enter maintenance mode before remediation. If you enable vSphere Lifecycle Manager to retry to put the host in maintenance mode, you must specify the number of retries and the retry delay. vSphere Lifecycle Manager waits for as much time as you configure for the **Retry Delay** option, and retries to put the host in maintenance mode as many times as you indicate in the **Number of retries** text box.
PXE booted hosts	You can allow the installation of software for solutions on the PXE booted ESXi hosts in the vSphere inventory that you manage withvSphere Lifecycle Manager baselines.
VM migration	If you enable virtual machine migration by selecting the respective option, vSphere Lifecycle Manager migrates the suspended and powered off virtual machines from the hosts that must enter maintenance mode to other hosts in the cluster.
Removable media devices	vSphere Lifecycle Manager does not remediate hosts on which virtual machines have connected CD/DVD or floppy drives. All removable media drives that are connected to the virtual machines on a host might prevent the host from entering maintenance mode and interrupt remediation. So, you can disconnect all removable media devices to ensure that the respective host enters maintenance mode successfully. After remediation, vSphere Lifecycle Manager reconnects the removable media devices if they are still available.
Quick Boot	Quick Boot reduces the host reboot time during remediation. By default, Quick Boot is deactivated.
Parallel remediation	Enabling parallel remediation allows you to remediate multiple ESXi hosts simultaneously. By selecting the **Parallel remediation** option, you enable vSphere Lifecycle Manager to remediate all hosts that are in maintenance mode in parallel instead of in sequence. Alternatively, you can specify the maximum number of concurrent remediations manually. **Note** If the hosts have NSX virtual distributed switches that are ready to be migrated to vSphere Distributed Switches, you must manually set the maximum number of parallel remediations to no more than 4. In cases when host switch migration is needed, if more than 4 hosts are remediated in parallel, the remediation might fail, because the host switch migration takes more time than the time vSphere Lifecycle Manager needs to complete the parallel remediation.

Results

These settings become the default failure response settings with vSphere Lifecycle Manager baselines. You can specify different settings when you configure individual remediation tasks.

Configure vSphere Lifecycle Manager Remediation Settings for vSAN Clusters that You Manage with vSphere Lifecycle Manager Baselines

You can configure what type of baseline to include in the recommendation baseline group that vSphere Lifecycle Manager generates for a vSAN cluster.

A recommendation baseline group can contain upgrades or only host patches and updates. By default, vSphere Lifecycle Manager is set to generate recommendation baselines that contain upgrades, not only patches and updates. However, you can change the default configuration at any time. For any vSAN cluster that you manage with baselines, you can also configure vSphere Lifecycle Manager to generate no recommendation baseline group at all. In such cases, you can still manually create baselines and perform host upgrades.

Prerequisites

- Verify that you manage the vSAN cluster with vSphere Lifecycle Manager baselines and not a single vSphere Lifecycle Manager image.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a vSAN cluster that you manage with baselines.
2. On the **Updates** tab, select **Hosts > Cluster Settings**.
3. In the **Remediation Settings for this Cluster** pane, click the **Edit** button.

   The **Edit Cluster Remediation Settings** dialog box appears.
4. Select what type of baseline to include in the recommendation baseline group that vSphere Lifecycle Manager generates for the selected vSAN cluster.
   - To include upgrade baselines into the recommendation baseline group for that cluster, select the **Include upgrades to new ESXi versions** radio button.

     The **Include upgrades to new ESXi versions** options is the default selection for any newly created vSAN cluster.
   - To include only patches and updates in the recommendation baseline group for that cluster, select the **Include patches and updates for current ESXi version** radio button.
   - To stop the generation of the recommendation baseline group for that cluster, select the **No recommendation** baseline group.
5. Click the **Done** button to save your selection and exit the dialog box.

   The option that you select becomes the default configuration for the vSAN cluster.

Creating and Managing vSphere Lifecycle Manager Clusters

4

A vSphere Lifecycle Manager cluster is a cluster of ESXi hosts that you manage either with baselines or with a single image. You decide whether to manage a cluster with baselines or with a single image during the creation of the cluster.

Creating a vSphere Lifecycle Manager Cluster That Uses a Single Image

When you create a cluster, the option to use a single image for that cluster is selected by default. You must keep it selected unless you want to create a cluster that uses baselines. During cluster creation, you must set up an image yourself or use the image of a host within or outside the current vCenter Server instance. In both cases, you can also enable vSphere Configuration Profiles for the cluster that you create.

Starting with vSphere 8.0, the default selections in the **New Cluster** wizard are based on the presumption that you are creating a cluster that uses a single image.

Creating a vSphere Lifecycle Manager Cluster That Uses Baselines

To create a cluster that uses baselines, during cluster creation, you deselect the option to manage the cluster with a single image. You can switch from using baselines to using images at a later time. For more information about switching from using baselines to using images, see Convert a Cluster or a Host That Uses Baselines Into a Cluster or a Host That Uses vSphere Lifecycle Manager Images.

Adding Hosts to a vSphere Lifecycle Manager Cluster

You can add hosts of any version to a cluster that you manage with baselines.

You can add hosts of ESXi version 7.0 or later to a cluster that you manage with a single image. You can add a host to a cluster and at the same time use the image on that host as an image for the entire cluster.

Removing Hosts from a vSphere Lifecycle Manager Cluster

Removing a host from a cluster is a straightforward procedure. If you remove a host from a cluster that uses a single image, the host retains the software and firmware installed during the last remediation against the image for the cluster.

Note When you remove a host from a vSAN cluster that you manage with a single image, vSphere Lifecycle Manager invalidates the results from the last hardware compatibility check for the cluster. To obtain valid hardware compatibility information about the cluster, you must re-run a hardware compatibility check. For instructions on how to check the hardware compatibility for a cluster, see Check the Hardware Compatibility of a Cluster .

All cluster-related operations are described in full detail in the *vCenter Server and Host Management* documentation.

For information about using Auto Deploy to deploy and provision ESXi hosts, see the *VMware ESXi Installation and Setup* documentation.

Read the following topics next:

- Create a Cluster That Uses a Single Image by Composing a New Image
- Create a Cluster That Uses a Single Image by Importing an Image from a Host
- Add Hosts to a Cluster that Uses a Single Image

Create a Cluster That Uses a Single Image by Composing a New Image

You can create a vSphere Lifecycle Manager cluster that uses a single image by setting up the desired image during the creation of the cluster. When you choose to set up the image manually instead of importing it from a host, you must have the necessary software available in the vSphere Lifecycle Manager depot.

When you set up an image manually, you must specify the ESXi version for the image and, optionally, a vendor add-on. After the cluster creation is complete, you can further customize the image. For example, you can add components to the image. You can also configure a hardware support manager and add a firmware and drivers add-on to the image. For information about editing an image, see Edit a vSphere Lifecycle Manager Image.

If you decide to enable vSphere Configuration Profiles on the cluster, you must set up the host configuration manually after you complete the cluster creation.

Prerequisites

- Review the requirements for using a single image in What Are the Requirements for Using vSphere Lifecycle Manager.
- Verify that the hosts are of ESXi version 7.0 or later.
- Verify that a data center exists in the vCenter Server inventory.

- Verify that you have an ESXi image available in the vSphere Lifecycle Manager depot.
- If you want to enable vSphere Configuration Profiles on the cluster, verify that the following requirements are met:
  - You have the required license.
  - The hosts in the cluster are of ESXi version 8.0 or later.
  - vCenter Server is version 8.0 or later.

Procedure

1. In the vSphere Client, navigate to the **Hosts and Clusters** inventory.
2. Right-click a data center and select **New Cluster**.

   The **New Cluster** wizard opens.
3. On the **Basics** page, enter a name for the cluster and enable vSphere DRS, vSphere HA, or vSAN.
4. Leave the **Manage all hosts in the cluster with a single image** check box and **Compose a new image** radio button selected.

   Those options are selected by default.
5. (Optional) To enable vSphere Configuration Profiles on the cluster, select the **Manage configuration at a cluster level**.
6. Click **Next**.
7. On the **Image** page, set up the desired image.
   a. Select an ESXi version.
   b. (Optional) Select a vendor add-on and the version of the add-on.
8. Click **Next**.
9. On the **Review** page, review your selections and the image setup.
10. Click **Finish** to finish the creation of the cluster.

Results

A cluster that uses a single image appears in the vCenter Server inventory. You can view and customize the cluster image on the **Updates** tab for the cluster.

If the cluster has vSphere Configuration Profiles enabled, you can configure the settings of the hosts in the cluster collectively by going to the **Configure** tab for the cluster and clicking **Desired State > Configuration**. See Edit the Host Settings of a Draft Configuration in vSphere Client.

What to do next

Add hosts to the cluster.

Create a Cluster That Uses a Single Image by Importing an Image from a Host

During cluster creation, instead of composing a new image, you can import the desired software specification from a reference host. If you choose to import an image, vSphere Lifecycle Manager extracts the software specification from the reference host and uses it for the newly created cluster. Importing an image saves you the time and effort of ensuring that you have all necessary components and images available in the vSphere Lifecycle Manager depot. Also, because you use a ready-made image, you do not need to spend time validating the new image.

During image import, along with extracting the software specification from the reference host, vSphere Lifecycle Manager also extracts the software depot associated with the image, and imports the software components to the vSphere Lifecycle Manager depot in the vCenter Server instance where you create the cluster. As a result, in air-gap scenarios, you only need one reference host to obtain the necessaryESXi image and components in the local depot and to create a software specification for your clusters.

You can import an image from an ESXi host that is in the same or a different vCenter Server instance. You can also import an image from an ESXi host that is not managed by vCenter Server. The reference host can also be in a cluster that you manage with baselines. Along with importing the image, you can also choose to move the reference host to the cluster. As a result, the newly created cluster uses the same image as the image on the reference host, which is now part of that cluster. If the reference host is in another vCenter Server instance, you can import the image from that host, but you cannot move it to the cluster.

Note When you import an image from a host, vSphere Lifecycle Manager retrieves the ESXi version, vendor add-on, and user-added components from the host. vSphere Lifecycle Manager does not extract the components from solutions and firmware updates installed on the reference host. Therefore, the image for the new cluster does not contain solution components or a firmware and drivers add-on. To obtain firmware updates in the depot and add a firmware and drivers add-on to your cluster image, you must configure a hardware support manager for the cluster after the cluster is created. For more information about firmware updates, see Firmware Updates with vSphere Lifecycle Manager.

In vSphere 8.0, you can use the image of a reference host that is in a DPU-based cluster and import it into a non-DPU cluster. Similarly, you can select a non-DPU host as the reference host for a DPU-based cluster.

Prerequisites

- Verify that the vCenter Server version is 7.0 Update 2
- Verify that a data center exists in the vCenter Server inventory.
- Verify that the reference host is version ESXi 7.0 Update 2 or later.
- Obtain the user name and password of the root user account for the reference host if it is not in your vCenter Server instance.

- Review the requirements for using a single image in What Are the Requirements for Using vSphere Lifecycle Manager.
- If you want to enable vSphere Configuration Profiles on the cluster, verify that the following requirements are met:
  - You have the required license.
  - The hosts in the cluster are of ESXi version 8.0 or later.
  - vCenter Server is version 8.0 or later.

Procedure

1. In the vSphere Client, navigate to the **Hosts and Clusters** inventory.
2. Right-click a data center and select **New Cluster**.

   The **New Cluster** wizard opens.
3. On the **Basics** page, enter a name for the cluster and enable vSphere DRS, vSphere HA, or vSAN.
4. Leave the **Manage all hosts in the cluster with a single image** check box selected.

   This option is selected by default.
5. Choose the import method of creating an image for the cluster.
   - To import an image from a host that is in the same vCenter Server inventory, select the **Import image from an existing host in the vCenter inventory** radio button.
   - To import an image from a host that is in a different vCenter Server instance or a standalone host that is not added to your vCenter Server, select the **Import image from a new host** radio button.
6. (Optional) To enable vSphere Configuration Profiles on the cluster, select the **Manage configuration at a cluster level** check box.
7. Click **Next**.

8 Select the host image you want to import and use for the cluster.

Import Option	Steps
Import an image from an existing host in the vCenter Server inventory	a On the **Select Image** page, select the reference host which you want to extract the image from and click **Next**. **Note** After you select a reference host, detailed information about the image on the selected host appears at the bottom of the page. You can view the ESXi version and all additional components.
Import an image from a new host	a On the **Image** page, enter the host details and click the **Find Host** button. b If a **Security Alert** dialog box appears, click **Yes** to confirm that you want to connect to the host. c To move a standalone host to the cluster, select the **Also move selected host to cluster** check box and click **Next**.

9 On the **Review** page, review your selections and verify that the selected reference host and its image are what you need.

10 Click **Finish**.

Results

A cluster that uses a single image appears in the vCenter Server inventory. Depending on your selections, the reference host might be in the newly created cluster. The image for that cluster is identical to the image on the selected reference host. You can view and customize the cluster image on the **Updates** tab for the cluster.

If the cluster has vSphere Configuration Profiles enabled, you can configure the settings of the hosts in the cluster collectively by going to the **Configure** tab for the cluster and clicking **Desired State > Configuration**. See Edit the Host Settings of a Draft Configuration in vSphere Client.

What to do next

Add other hosts to the cluster.

Add Hosts to a Cluster that Uses a Single Image

When you add hosts to a cluster, you can appoint one of those hosts as a reference host. vSphere Lifecycle Manager extracts and uses the image on the reference host as the new image for the cluster. The option to import a host's image to the cluster facilitates and simplifies the cluster upgrade operation by removing the need for you to manually import components to the vSphere Lifecycle Manager depot, set up and validate a new image, check the compliance of the hosts against the image, and then remediate the cluster against the image to apply the new software specification to all hosts.

Along with extracting the software specification from the appointed reference host, vSphere Lifecycle Manager also extracts the software depot associated with the image, and imports the components to the vSphere Lifecycle Manager depot in the vCenter Server instance where the target cluster is.

Note When you import an image from a host, vSphere Lifecycle Manager retrieves the ESXi version, vendor add-on, and user-added components from the host. vSphere Lifecycle Manager does not extract the components from solutions and firmware updates installed on the reference host. Therefore, the new image for the cluster does not contain solution components or a firmware and drivers add-on. To obtain firmware updates in the depot and add a firmware and drivers add-on to your cluster image, you must configure a hardware support manager. For more information about firmware updates, see Firmware Updates with vSphere Lifecycle Manager.

Adding a host to a cluster and importing its image to the target cluster changes the compliance state of the other hosts in the cluster. After adding the host and setting its image as the new cluster image, you can run a compliance check. The newly added host is compliant against the new cluster image. The rest of the hosts become non-compliant. To apply the new cluster image to all the hosts in the cluster and make them compliant, you must remediate the cluster.

Note You cannot downgrade the software that is actually installed on the hosts in the cluster. If the image on the reference host contains software components of lower version, you can still import and use that image for the cluster. However, the hosts in the cluster become incompatible with the new image, and you cannot proceed and remediate the cluster against that image.

Prerequisites

- Verify that the vCenter Server version is 7.0 or later.
- Verify that the hosts to add are of version ESXi 7.0 or later.
- Verify that the hosts that you add to the cluster are of the same main and patch version as the rest of the hosts.
- Obtain the user name and password of the root user account for the hosts that are not in your vCenter Server instance.
- Review the requirements for using a single image in What Are the Requirements for Using vSphere Lifecycle Manager.
- To add a host and import its image to the cluster, verify that the following requirements are met.
  - The vCenter Server instance is of version 7.0 Update 2 or later.
  - The ESXi version on the reference host is 7.0 Update 2 or later.
- To add a host to a cluster that has vSphere Configuration Profiles enabled, verify that the following requirements are met.
  - The vCenter Server instance is of version 8.0 or later.

- The ESXi version of the host 7.0 Update 3 or later.
- The host doesn't have NSX or vSphere Distributed Switch configured.
- No host profile is attached to the host.

Procedure

1 In the vSphere Client, navigate to the **Hosts and Clusters** inventory.

2 Right-click cluster and select **Add Hosts**.

   The **Add Hosts** wizard opens.

3 On the **Add hosts**, specify the hosts that you want to add to the cluster and click **Next**.

   - Add a host that is not in the same vCenter Server inventory.

     a Click the **New Hosts** tab.

     b Enter the required information about the host in the text boxes.

     c To add more new hosts, click the **Add Host** button and enter the required information.

     d Select the **Use the same credentials for all hosts** check box.

   - Add a host that is in the same vCenter Server inventory.

     a Click the **Existing hosts** tab.

     b Select one or multiple hosts from the list.

   Note If you want to add multiple hosts, you do not need to specify only new hosts or only existing hosts. You can specify new hosts and select from the existing hosts at the same time.

4 On the **Host Summary** page, review the information about the hosts and click **Next**.

5 On the **Import Image** page, select the host whose image to use as the image for the cluster.

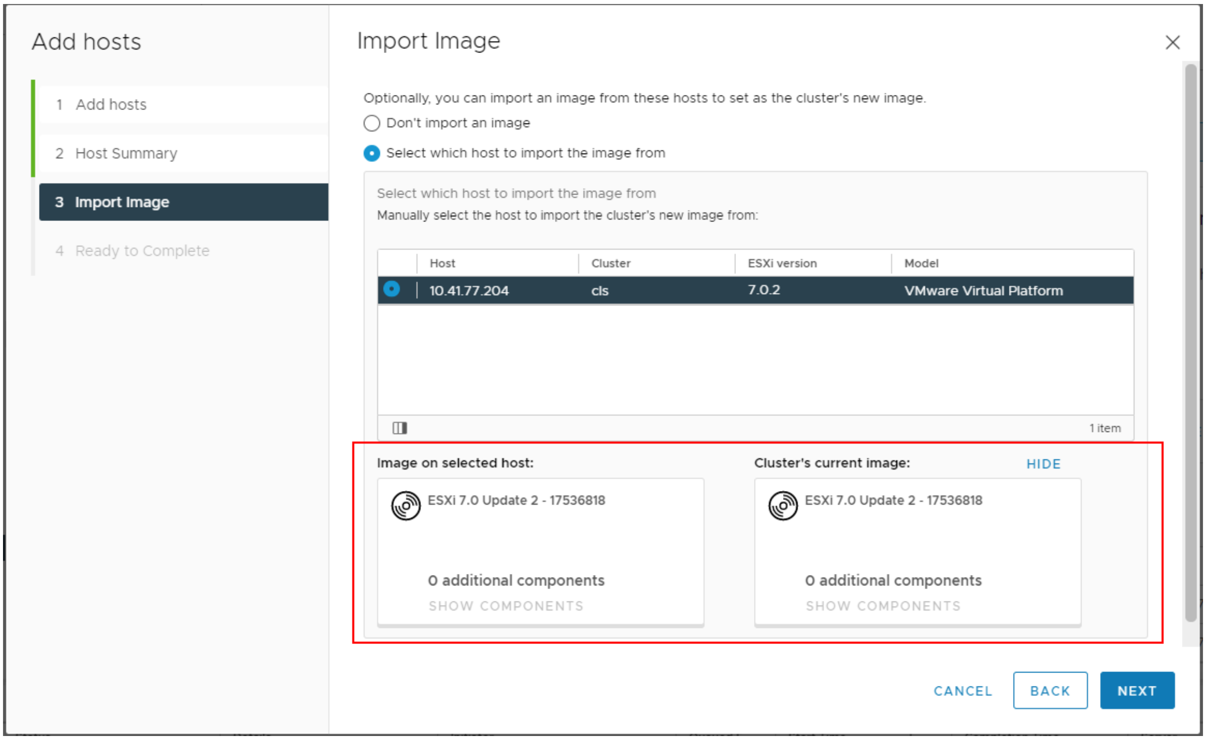
   - To add the specified hosts to the cluster without changing the current image for that cluster, select the **Don't import an image** radio button.
   - To use any of the specified hosts as a reference host and use its image as the new image for that cluster, select the **Select which host to import the image from** radio button and select a host from the list.

     Note If the image on the host that you select is of version earlier than ESXi 7.0 Update 2, you cannot proceed with importing the image from that host.

   When you select a host to import an image from, a card with information about the image appears. you can view the ESXi version, the vendor add-on, and the additional components that the image on the reference host contains.

6 If you selected the **Select which host to import the image from** radio button, click **Show Cluster's Current Image** at the bottom of the page.

A card with information about the current image for the cluster appears. Before you proceed, you can review and compare the current cluster image with the image on the selected host before you proceed. In this way, you can ensure that you selected the right reference host.



7 Click **Next**.

8 On the **Ready to Complete** page, review the information about the selected hosts and the new cluster image.

9 Click **Finish** to add the hosts to the cluster.

Results

The specified hosts are added to the cluster.

If you chose to import an image from a host during the host addition procedure, the image for the cluster changes. The new software specification for the cluster is identical to the one on the selected and added reference host.

What to do next

If you chose to import an image from a host during the host addition procedure, remediate the cluster to apply the new image to all the hosts.

Managing Standalone ESXi Hosts with vSphere Lifecycle Manager Images 5

Starting with vSphere 8.0, you can use an image to manage the lifecycle of any standalone ESXi host that is part of your vCenter Server inventory. In vSphere 8.0 Update 1, you can use both, the vSphere Client and the vSphere Automation API, to manage the lifecycle of a standalone host.

A standalone host is a host that is connected to a vCenter Server instance but is not part of any cluster. In your inventory, standalone hosts are the hosts directly under a data center object or in a host folder.

The permissions and privileges that you need to manage a standalone host with an image are the same as the vSphere Lifecycle Manager permissions and privileges that you need for the respective operations at a cluster level.

No limits exist for the number of standalone hosts that you can manage with vSphere Lifecycle Manager images. The real limit is the number of hosts that vCenter Server can support.

By using the vSphere Client and the vSphere Automation API commands, you can start using images on a standalone host that you already manage with baselines. When you take a host out of a cluster that you manage with vSphere Lifecycle Manager image, the host does not retain the image. The host becomes managed by baselines. The reverse action, moving a standalone host that you manage with an image to a cluster that you manage with a single image is not supported.

In vSphere 8.0 Update 1, you can perform on standalone hosts all vSphere Lifecycle Manager operations that you can perform at a cluster level by using the vSphere Client or the respective API commands.

When you add a standalone host to a data center or a folder, the option to use a vSphere Lifecycle Manager image for the host is selected by default. You must keep it selected unless you want to manage the lifecycle of that standalone host with baselines. During the addition of the standalone host, you can either set up an image manually, use the existing image on the host, or import an image from a reference host in the vCenter Server inventory. For information, see Set Up a New Image to a Host When Adding the Host to a Data Center or Folder , Import an Image from a Reference Host When Adding a Host to a Data Center or Folder , and Use the Current Image of a Host When Adding the Host to a Data Center or Folder.

After the standalone host is added to the data center or folder, you can further customize the image. For more information, see Edit a vSphere Lifecycle Manager Image.

For information about how to convert an existing standalone host to a host that is managed with a vSphere Lifecycle Manager image and all available workflows for managing a standalone host with images, see Chapter 6 How to Use vSphere Lifecycle Manager Images .

Read the following topics next:

- Use the Current Image of a Host When Adding the Host to a Data Center or Folder
- Import an Image from a Reference Host When Adding a Host to a Data Center or Folder
- Set Up a New Image to a Host When Adding the Host to a Data Center or Folder

Use the Current Image of a Host When Adding the Host to a Data Center or Folder

When you add a standalone host to a data center or folder in vCenter Server, you can use the current image on the host to manage its lifecycle.

During the addition of a standalone host to a data center or a folder, you can choose to import an image from a host in the inventory and use this image to manage the lifecycle of the host. After the standalone host is added to the data center or folder, you can further customize the image. For example, you can customize the additional components or configure a hardware support manager and add firmware and drivers add-ons to the image. For information about editing an image, see Edit a vSphere Lifecycle Manager Image.

Prerequisites

- Review the requirements for using a single image in What Are the Requirements for Using vSphere Lifecycle Manager.
- Verify that a data center or a folder exists in the inventory.
- Verify that the vCenter Server instance is version 8.0 Update 3 or later.
- Verify that the host is of ESXi version 7.0 or later.
- Obtain the user name and password of the root user account for the host.
- Verify that you have an ESXi image available in the vSphere Lifecycle Manager depot.
- Verify that you have the proper privileges. For more information, see vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a data center or folder within a data center.

2 Right-click the data center or folder and select **Add Host**.

   The **Add Host** wizard opens.

3 On the **Name and location** page, enter the IP address or the name of the host and click **Next**.

4 On the **Connection settings** page, enter administrator credentials and click **Next**.

5 On the **Host summary** page, review the host summary and click **Next**.

6 On the **Host lifecycle** page, leave the **Manage host with an image** check box selected.

   This option is selected by default.

7 Select the **Import image from an existing host in the vCenter inventory** radio button and click **Next**.

8 On the **Select image** page, select the reference host which you want to extract the image from and click **Next**.

   After you select the reference host, detailed information about the image appears at the bottom of the page. You can view the ESXi version and all additional components.

9 On the **Assign license** page, add a license to the host and click **Next**.

10 (Optional) On the **Lockdown mode** page, select a lock-down mode option to deactivate the remote access for the administrator account after vCenter Server takes control of this host and click **Next**.

11 On the **VM location** page, select a location for the virtual machines that reside on the host and click **Next**.

12 On the **Ready to complete** page, review your selections and the image setup and click **Finish**.

Results

A standalone host that uses a vSphere Lifecycle Manager image appears in the vCenter Server inventory.

What to do next

View and customize the host image on the **Updates** tab for the standalone host.

Import an Image from a Reference Host When Adding a Host to a Data Center or Folder

When you add a standalone host to a data center or folder, you can import an image from another host in vCenter Server to manage the host lifecycle.

When you add a standalone host to a data center or a folder, you can use the image that is currently present on the host. After the standalone host is added to the data center or folder, you can further customize this image. For example, you can add additional components or configure a hardware support manager and add firmware and drivers add-ons to the image. For information about editing an image, see Edit a vSphere Lifecycle Manager Image.

Prerequisites

- Review the requirements for using a single image in What Are the Requirements for Using vSphere Lifecycle Manager.
- Verify that a data center or a folder exists in the inventory.

- Verify that the vCenter Server instance is version 8.0 Update 3 or later.
- Verify that the host is of ESXi version 7.0 or later.
- Obtain the user name and password of the root user account for the host.
- Verify that you have an ESXi image available in the vSphere Lifecycle Manager depot.
- Verify that you have the proper privileges. For more information, see vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a data center or folder within a data center.

2 Right-click the data center or folder and select **Add Host**.

  The **Add Host** wizard opens.

3 On the **Name and location** page, enter the IP address or the name of the host and click **Next**.

4 On the **Connection settings** page, enter administrator credentials and click **Next**.

5 On the **Host summary** page, review the host summary and click **Next**.

6 On the **Host lifecycle** page, leave the **Manage host with an image** check box selected.

  This option is selected by default.

7 Select the **Use the current image on host** radio button and click **Next**

  After you select this option, detailed information about the image on the host appears on this page. You can view the ESXi version and all additional components.

8 On the **Assign license** page, add a license to the host and click **Next**.

9 (Optional) On the **Lockdown mode** page, select a lock-down mode option to deactivate the remote access for the administrator account after vCenter Server takes control of this host and click **Next**.

10 On the **VM location** page, select a location for the virtual machines that reside on the host and click **Next**.

11 On the **Ready to complete** page, review your selections and the image setup and click **Finish**.

Results

A standalone host that uses a vSphere Lifecycle Manager image appears in the vCenter Server inventory.

What to do next

View and customize the host image on the **Updates** tab for the standalone host.

Set Up a New Image to a Host When Adding the Host to a Data Center or Folder

You can add a standalone host to a data center or folder and set up a new vSphere Lifecycle Manager image to manage the lifecycle of the host.

When you add a standalone host to a data center or a folder, you must specify the ESXi version for the image and, optionally, a vendor add-on. After the standalone host is added to the data center or folder, you can further customize the image. For example, you can add components to the image. You can also configure a hardware support manager and add a firmware and drivers add-on to the image. For information about editing an image, see Edit a vSphere Lifecycle Manager Image.

Prerequisites

- Review the requirements for using a single image in What Are the Requirements for Using vSphere Lifecycle Manager.
- Verify that a data center or a folder exists in the inventory.
- Verify that the host is of ESXi version 7.0 or later.
- Obtain the user name and password of the root user account for the host.
- Verify that you have an ESXi image available in the vSphere Lifecycle Manager depot.
- Verify that you have the proper privileges. For more information, see vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a data center or folder within a data center.

2 Right-click the data center or folder and select **Add Host**.

   The **Add Host** wizard opens.

3 On the **Name and location** page, enter the IP address or the name of the host and click **Next**.

4 On the **Connection settings** page, enter administrator credentials and click **Next**.

5 On the **Host summary** page, review the host summary and click **Next**.

6 On the **Host lifecycle** page, leave the **Manage host with an image** check box and the **Compose a new image** radio button selected.

   These options are selected by default.

7 Click **Next**.

8 On the **Image** page, set up the desired image and click **Next**.

   a Select an ESXi version.

   b (Optional) Select a vendor add-on and the version of the add-on.

9 On the **Assign license** page, add a license to the host and click **Next**.

10 (Optional) On the **Lockdown mode** page, select a lock-down mode option to deactivate the remote access for the administrator account after vCenter Server takes control of this host and click **Next**.

11 On the **VM location** page, select a location for the virtual machines that reside on the host and click **Next**.

12 On the **Ready to complete** page, review your selections and the image setup and click **Finish**.

Results

A standalone host that uses a single image appears in the vCenter Server inventory. You can view and customize the host image on the **Updates** tab for the standalone host.

How to Use vSphere Lifecycle Manager Images

6

Using vSphere Lifecycle Manager images provides a simplified and unified workflow for patching and upgrade of ESXi hosts. You can also use vSphere Lifecycle Manager images for bootstrapping purposes and firmware updates.

An image defines the exact software stack to run on all ESXi hosts in a cluster or on a standalone host.

General Workflow

Using images to apply software and firmware updates to ESXi hosts is a multi-stage process.

1 Software updates must become available in the vSphere Lifecycle Manager depot.

   To set up and use an image, you use the software updates that are available in the vSphere Lifecycle Manager depot. The depot contains base images, vendor add-ons, and additional components.

   Updates get into the vSphere Lifecycle Manager local depot through synchronization with configurable download sources. By default, vSphere Lifecycle Manager is configured to synchronize with the official VMware depot. You can also import updates into the depot manually.

   You can see the contents of the vSphere Lifecycle Manager depot in the vSphere Lifecycle Manager home view.

   For more information, see Chapter 2 The vSphere Lifecycle Manager Depot.

2 Start using vSphere Lifecycle Manager images.

   vSphere Lifecycle Manager provides you with the option to start using images during the procedure for creating a cluster or adding a host to a data center or folder. If you do not set up an image during the creation of a cluster or the addition of a standalone host, you can switch from using vSphere Lifecycle Manager baselines to using vSphere Lifecycle Manager images at a later time.

   Even when you save the image, no software is installed on the ESXi hosts during image setup.

For more information, see Chapter 4 Creating and Managing vSphere Lifecycle Manager Clusters, Chapter 5 Managing Standalone ESXi Hosts with vSphere Lifecycle Manager Images, and Convert a Cluster or a Host That Uses Baselines Into a Cluster or a Host That Uses vSphere Lifecycle Manager Images.

3 Check the compliance of the ESXi hosts in the cluster or the standalone host against the image specification.

   The compliance check compares the current image on the ESXi hosts in the cluster or the standalone host against the desired image that you specified during the setup process, and defines compatibility status of the hosts.

   For more information, see Check the Compliance of a Cluster Against a vSphere Lifecycle Manager Image and View Host Compliance Information .

4 Review the compliance statuses of the hosts in the cluster or the standalone host.

5 You can run a remediation pre-check on an ESXi host to ensure software and hardware compatibility with the image.

   Running a remediation pre-check is optional. The remediation pre-check ensures that all requirements for successful remediation are met. For more information, see Run a Remediation Pre-Check for a Cluster, a Host Within a Cluster, or a Standalone Host.

6 Remediate the non-compliant ESXi hosts in the cluster or the non-compliant standalone host.

   Remediation is the process through which the software specification defined by the vSphere Lifecycle Manager image that you use for a cluster or a host is actually applied to the hosts in the cluster or to the standalone host.

   For more information about remediating hosts against an image, see Remediating a Cluster or a Standalone Host Against a Single Image.

Limitations

- When you set up and save an image for a cluster or a standalone host, the image is not applied to the hosts in the cluster or to the standalone host unless you remediate the hosts. The mere action of changing the management method does not alter the hosts in the cluster or the standalone host.
- After you set up an image for the cluster or the standalone host and remediate the hosts in the cluster or the standalone host against the image, standalone VIBs are deleted from the hosts.
- After you set up an image for the cluster or the standalone host and remediate the hosts in the cluster or the standalone host against the image, non-integrated solution agents are deleted from the hosts.

Read the following topics next:

- Convert a Cluster or a Host That Uses Baselines Into a Cluster or a Host That Uses vSphere Lifecycle Manager Images

- Working with Images
- Check the Compliance Against a Single Image
- Staging vSphere Lifecycle Manager Images to ESXi Hosts in a Cluster or Standalone Hosts
- Run a Remediation Pre-Check for a Cluster, a Host Within a Cluster, or a Standalone Host
- Remediating a Cluster or a Standalone Host Against a Single Image
- View Last Remediation or Remediation Pre-Check Results for a Cluster or a Standalone Host that Uses a Single Image
- Manage Depot Overrides for a Cluster or a Standalone Host
- vSphere Lifecycle Manager Recommended Images
- Firmware Updates with vSphere Lifecycle Manager

Convert a Cluster or a Host That Uses Baselines Into a Cluster or a Host That Uses vSphere Lifecycle Manager Images

You can manage a cluster or a standalone host with either baselines or images. You cannot use both at the same time for a single cluster or host. Even if you do not set up an image for the cluster during cluster creation or for the host when adding it to the data center or folder, you can at any time switch from using baselines to using images for that cluster or host.

To switch a cluster to vSphere Lifecycle Manager images, you must set up a new image or import an existing one. In vSphere 8.0 Update 1, to switch a standalone host to a vSphere Lifecycle Manager images, you can either set up a new image or import an existing one. Before you proceed with setting up or importing an image, vCenter Server checks and reports if the cluster or host is eligible for using images. For more information about cluster or host eligibility, see Cluster or Standalone Host Eligibility to Use vSphere Lifecycle Manager Images.

System Requirements

To switch to using images, the cluster or host must meet multiple requirements.

- All ESXi hosts in the cluster or the standalone host must be of version 7.0 and later.
- All ESXi hosts in the cluster or the standalone host must be stateful.

  A stateful install is one in which the host boots from a disk.
- No host in the cluster or standalone host can contain any unknown components.

If a host is of version earlier than ESXi 7.0, you must first use an upgrade baseline to upgrade the host and then you can successfully switch to using images. For more information about using baselines for host patching and upgrade operations, see Chapter 8 Using vSphere Lifecycle Manager Baselines and Baseline Groups .

For more information about converting a stateless host into a stateful host, find information about Auto Deploy in the *VMware ESXi Installation and Setup* documentation.

Specifics of the Transitioning Workflow

Several behavioral specifics exist when you switch to using vSphere Lifecycle Manager images.

- If you switch to using images, you cannot revert to using baselines for the cluster. You can move the hosts to a cluster that uses baselines, but you cannot change a cluster that already uses a single image for management purposes.
- If you switch to using images for a standalone host, you cannot revert to using baselines for the host except if you re-add the standalone host to the vCenter Server inventory.
- When you set up and save an image for a cluster or host, the image is not applied to the hosts in the cluster or to the standalone host unless you remediate the hosts. The mere action of changing the management method does not alter the hosts in the cluster or the standalone host.
- After you set up an image for the cluster or the standalone host and remediate the hosts in the cluster or the standalone host against the image, standalone VIBs are deleted from the hosts.
- After you set up an image for the cluster or host and remediate the hosts in the cluster or the standalone host against the image, non-integrated solution agents are deleted from the hosts.
- If you enable a solution that cannot work with vSphere Lifecycle Manager, for example Dell EMC VxRail, on an empty cluster and attempt to switch to using an image for that cluster, the transition operation succeeds. However, the result is an unsupported cluster configuration, because both vSphere Lifecycle Manager and the non-integrated solution are enabled on the cluster.
- If you take a host out of a cluster that you manage with a vSphere Lifecycle Manager image, the host becomes standalone. The host can retain the image of the cluster in case the following criteria are met:
  - The vCenter Server and ESXi host are of version vSphere 8.0 Update 3 and later.
  - The host does not have the NSX component installed.
  - If the host contains the NSX component, NSX is of version 4.2 or later. See Using vSphere Lifecycle Manager Images for Standalone Hosts with NSX 4.2 and later.
  - During the move operation the host stays connected or reachable.

  Otherwise, the image is removed from the host and the host is reverted back to using baselines.

- The reverse action, moving a standalone host that you manage with a single image to a cluster that you manage with an image is supported. After you move the standalone host managed with a vSphere Lifecycle Manager image, you must check the compliance of the hosts in the cluster against the specified cluster image.

Cluster or Standalone Host Eligibility to Use vSphere Lifecycle Manager Images

Switching from baselines to images requires that you set up or import a vSphere Lifecycle Manager image to manage the cluster or host with. As part of the transition, before you set up the image, vCenter Server triggers an automatic task that checks whether the cluster or host is eligible to use vSphere Lifecycle Manager images.

The **Check cluster's eligibility to be managed with a single image** and **Check host's eligibility to be managed with a single image** tasks ensure that the cluster or host is not undergoing remediation against a baseline and check whether all requirements for using vSphere Lifecycle Manager images are met.

Also, the tasks check for standalone VIBs and ensure that no unintegrated solutions are enabled for the cluster or host. You might not be able to switch to using vSphere Lifecycle Manager images if unintegrated solutions are enabled on the cluster or host.

Note If you use any third-party products or solutions, you must confirm with your third-party software vendor whether the respective solution works with vSphere Lifecycle Manager.

The tasks return three types of notifications: error, warning, and info.

Errors

The **Check cluster's eligibility to be managed with a single image** and **Check host's eligibility to be managed with a single image** tasks report an error in case one of the following conditions occurs:

- The cluster contains at least one host that is not stateful or the standalone host is not stateful.
- The cluster contains at least one host that is not of a compatible ESXi version or the standalone host is of version different than 7.0 and later.
- The cluster or the standalone host contain VIBs of unintegrated solutions. In that case, you must deactivate the unintegrated solution and retry the transition.

Warnings

The **Check cluster's eligibility to be managed with a single image** and **Check host's eligibility to be managed with a single image** tasks issue a warning if the cluster contains at least one host with or the standalone host contains a standalone VIB or an unknown VIB. Warnings do not block the transition to using vSphere Lifecycle Manager images, but they require special attention or a user action.

For example, you see a warning notification if a host in the cluster contains a standalone VIB, for example a driver, for which a component is available in the vSphere Lifecycle Manager depot. If you want to keep the VIB, you must add the respective component to the vSphere Lifecycle Manager image. Otherwise, the standalone VIB is deleted upon remediation.

You also get a warning if a host in the cluster or the standalone host contain an unknown VIB. Unknown VIBs are standalone VIBs for which no component is available in the vSphere Lifecycle Manager depot. If vSphere Lifecycle Manager detects an unknown VIB, you must import a component that contains the VIB into the vSphere Lifecycle Manager depot and restart the transition. Otherwise, the unknown VIB is deleted upon remediation.

Info

The **Check cluster's eligibility to be managed with a single image** and **Check host's eligibility to be managed with a single image** tasks give an info notification if the cluster contains at least one host with a standalone VIB or the standalone host contains a standalone VIB, but you can still proceed to setting up a vSphere Lifecycle Manager image for the cluster or host without any additional actions.

For example, you see an info notification if the cluster is enabled for an integrated solution, for example vSphere HA or vSAN.

Option 1: Use an Image from a Host in the Cluster

To start managing an existing cluster or host that uses baselines with a single vSphere Lifecycle Manager image, you can select and use one of the images installed on a host in the cluster or the current image on the standalone host.

If you switch to using images, you cannot revert to using baselines for the cluster. You can move the hosts to another cluster, which uses baselines, but you cannot change the cluster that already uses a single image.

If you switch to using images for a standalone host, you cannot revert to using baselines for the host.

For conceptual information about vSphere Lifecycle Manager images, see vSphere Lifecycle Manager Images.

For information about how to use vSphere Lifecycle Manager images to manage hosts and clusters, see Chapter 6 How to Use vSphere Lifecycle Manager Images .

With vSphere 8.0 Update 3, instead of importing or manually setting up an image, you can use an image from a host that is already in the cluster or the image currently running on the standalone host.

When you initiate the transitioning workflow for a cluster that uses baselines, vSphere Lifecycle Manager triggers the **Get Installed Host Images** task after the eligibility checks finish successfully. During this task, vSphere Lifecycle Manager retrieves information about all images currently installed on the hosts in the cluster. Then vSphere Lifecycle Manager calculates which are the

most complete, valid, and suitable images that you can use to remediate the cluster. The list of suitable images is generated based on two criteria: the ESXi version and the software running on the hosts in the cluster. Based on these criteria, vSphere Lifecycle Manager provides the following image options to choose from:

- The image that contains the highest ESXi version.
- The image that has the most widely used software on most of the hosts in the cluster.
- The images that have a different software setup than the most widely used setup on the hosts in the cluster.

After you select an image from a host in the cluster, you can make changes to the image or save it without editing.

When you decide to add a host to or remove a host from a cluster that already has some generated list of suitable images, this list is invalidated. vSphere Lifecycle Manager automatically triggers a new **Get Installed Host Images** task. During this task, vSphere Lifecycle Manager retrieves information about the new set of images installed on the hosts in the cluster and computes a new list of suitable images based on the cluster membership changes. You can also regenerate the list of images at any time.

When you start converting a standalone host that uses baselines to a host that is managed with an image, you can view and use the image currently installed on the host. vSphere Lifecycle Manager automatically retrieves information about the current image on the standalone host. You can select and edit the current image on the standalone host or use it without changes.

Prerequisites

- Verify that all ESXi hosts in the cluster or the standalone host are of version 7.0 Update 2 and later.
- Verify that your vCenter Server instance is of version 8.0 Update 3 and later.
- Verify that all ESXi hosts in the cluster or the standalone host are stateful. A stateful install is one in which the host boots from a disk.
- Verify that all ESXi hosts in the cluster are from the same hardware vendor.
- Verify that no unintegrated solution is enabled for the cluster or the host.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

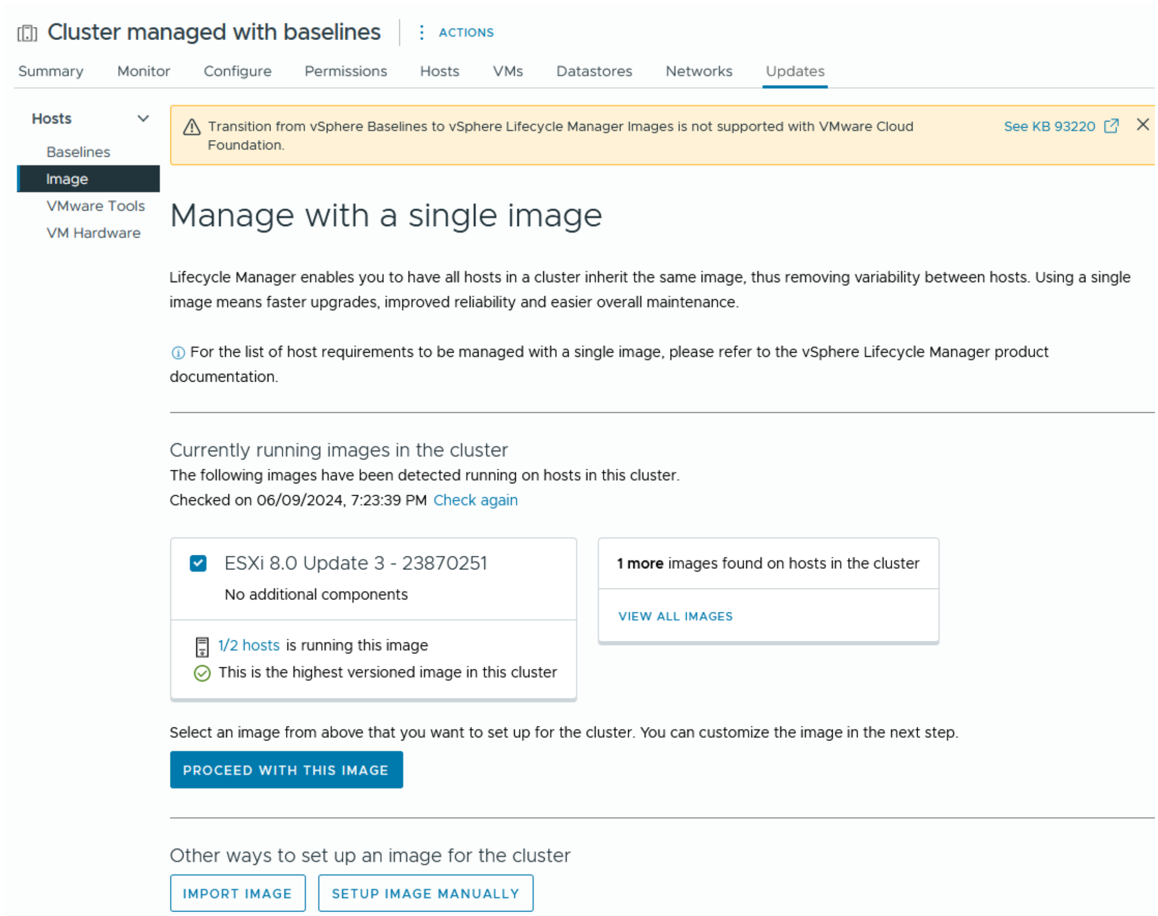
Procedure

1 In the vSphere Client, navigate to a cluster or host that you manage with baselines and baseline groups.

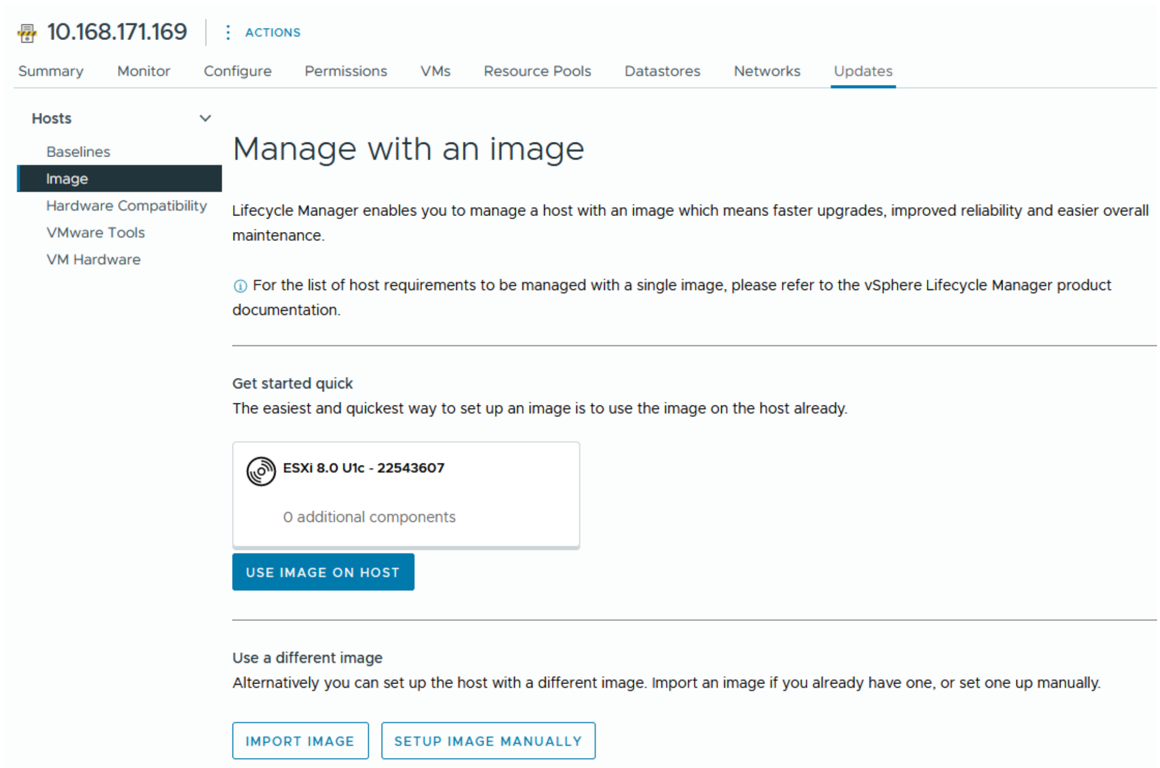
2 On the **Updates** tab, click **Image**.

vSphere Lifecycle Manager starts checking if the cluster or host is eligible for using images. If no problems are reported, vSphere Lifecycle Manager retrieves information about the images currently installed on the hosts in the cluster or the image running on the standalone host.

- If you selected a cluster, a list of the most valid and suitable images for the cluster is displayed in the **Currently running images in the cluster** page section.



- If you selected a standalone host, you can view the image card with details for the current host image in the **Get started quick** page section.



3 If you selected a cluster, select a host image from the provided list of images and click **Proceed with selected image** to confirm your selection.

   The **Convert to an Image** pane appears. The elements of the selected host image appear in the **Define Image** card.

4 If you selected a standalone host, click **Use image on host**.

   The **Convert to an Image** pane appears. The elements of the current host image appear in the **Define Image** card.

5 If you want to further customize the host image, edit any of the image elements.

6 (Optional) To validate the image, click the **Validate** button.

   You validate an image to check for missing dependencies and component conflicts.

7 Click **Save**.

   Saving the image triggers an automatic compliance check. All hosts in the cluster or the standalone host are checked against the image.

8 In the **Convert to an Image** pane, finish the image setup.

   a Click the **Finish image setup** button.

   b In the **Finish image setup** dialog box, click **Yes, finish image setup**.

Results

You now manage all hosts in the cluster collectively or the standalone host with a single image. Upon remediation, the image is installed on all hosts in the cluster or on the standalone host.

What to do next

To apply the image to all hosts in the cluster or the standalone host, remediate the cluster or host against the image.

Option 2: Import an Image from a JSON File

To start managing with a single vSphere Lifecycle Manager image an existing cluster or host that already uses baselines, you can import an image from another cluster or host instead of setting up a new image manually.

If you switch to using images, you cannot revert to using baselines for the cluster. You can move the hosts to another cluster, which uses baselines, but you cannot change the cluster that already uses a single image.

If you switch to using images for a standalone host, you cannot revert to using baselines for the host.

For conceptual information about vSphere Lifecycle Manager images, see vSphere Lifecycle Manager Images.

For information about how to use vSphere Lifecycle Manager images to manage hosts and clusters, see Chapter 6 How to Use vSphere Lifecycle Manager Images .

Prerequisites

- Verify that all ESXi hosts in the cluster or the standalone host are of version 7.0 and later.
- Verify that all ESXi hosts in the cluster or the standalone host are stateful. A stateful install is one in which the host boots from a disk.
- Verify that all ESXi hosts in the cluster are from the same hardware vendor.
- Verify that no unintegrated solution is enabled for the cluster or the host.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or host that you manage with baselines and baseline groups.

2 On the **Updates** tab, click **Image**.

3 Click the **Import Image** button.

   The **Import Image** dialog box appears.

4 Select a JSON file to import and click **Next**.

- Click the **Browse** button and select a JSON file on your local machine.
- Enter a valid URL to a JSON file on a remote web server.

vSphere Lifecycle Manager starts checking if the cluster or host is eligible for using images. If no problems are reported, the **Convert to an Image** pane appears. The elements of the imported image appear in the **Define Image** card.

5 (Optional) Customize the imported image by changing any of its elements.

6 (Optional) To validate the image, click the **Validate** button.

You validate an image to check for missing dependencies and component conflicts.

7 Click **Save**.

Saving the image triggers an automatic compliance check. All hosts in the cluster or the standalone host are checked against the image.

8 In the **Convert to an Image** pane, finish the image setup.

a Click the **Finish image setup** button.

b In the **Finish image setup** dialog box, click **Yes, finish image setup**.

Results

You now manage all hosts in the cluster collectively or the standalone host with a single image for the cluster or host. Upon remediation, the image is installed on all hosts in the cluster or on the standalone host.

What to do next

To apply the image to all hosts in the cluster or the standalone host, remediate the cluster or host against the image.

Option 3: Set Up a New Image Manually

You can start using vSphere Lifecycle Manager images for an existing cluster or host that uses baselines by setting up an image manually.

If you switch to using images, you cannot revert to using baselines for the cluster. You can move the hosts to another cluster, which uses baselines, but you cannot change the cluster that already uses a single image.

If you switch to using images for a standalone host, you cannot revert to using baselines for the host.

For conceptual information about vSphere Lifecycle Manager images, see vSphere Lifecycle Manager Images.

For information about how to use vSphere Lifecycle Manager images to manage hosts and clusters, see Chapter 6 How to Use vSphere Lifecycle Manager Images .

Prerequisites

- Verify that all ESXi hosts in the cluster or the standalone host are of version 7.0 and later.
- Verify that all ESXi hosts in the cluster or the standalone host are stateful. A stateful install is one in which the host boots from a disk.
- Verify that all ESXi hosts in the cluster are from the same hardware vendor.
- Verify that no unintegrated solution is enabled for the cluster or the host.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a cluster or host that you manage with baselines and baseline groups.
2. On the **Updates** tab, click **Image**.
3. Click the **Set up image manually** button.

   vSphere Lifecycle Manager starts checking if the cluster or host is eligible for using images. If no problems are reported, the **Convert to an Image** pane appears.
4. If the **Check cluster's eligibility to be managed with a single image** or **Check host's eligibility to be managed with a single image** tasks report an error or a warning that requires an action, resolve the issue and restart the procedure.
5. From the **ESXi Version** drop-down menu, select an ESXi image.
6. (Optional) Add a vendor add-on to the image.
   a. Click **Select**.

      The **Select Vendor Addon** appears.
   b. Select an add-on from the list.

      An information panel appears on the right. The information panel shows information about the components that the add-on adds to the ESXi image and the components that it removes from the image.
   c. From the **Version** column use the drop-down menu for the selected add-on and select the add-on version.
   d. Click **Select**.
7. (Optional) Add a firmware and drivers add-on to the image.
   a. Click **Select**.

      The **Select Firmware and Drivers Addon** appears.
   b. Select a hardware support manager from the respective drop-down menu.

      A list of firmware and drivers add-ons appears.

c Select an add-on from the list.

An information panel appears on the right. The information panel shows information about the supported ESXi versions and whether the add-on contains a driver or not.

d From the **Version** column use the drop-down menu for the selected add-on and select the add-on version.

e Click **Select**.

8 (Optional) Manage the additional components of the image.

a Click **Show details**.

b Click **Add components**.

The **Add Components** dialog box appears.

c (Optional) Use the **Show** drop-down menu to sift out the components that are not part of the selected vendor add-on.

d Select one or multiple components from the list.

An information panel appears on the right. The information panel shows information about the component that you selected first.

e From the **Version** column use the drop-down menu for the selected component to select the component version.

Caution If your vCenter Server instance and all ESXi hosts in the cluster are of version 8.0 Update 3 or later, you can select and retain a lower version for an additional component that is part of the ESXi base image. To avoid critical errors on any of the hosts in the cluster, make sure you perform thorough testing of the customized image before remediating the cluster.

f Click **Select**.

The selected components appear in the list of components that the image contains. You can use the **Show** drop-down menu to sift out the additional components. For example, you can list only the customized components.

g (Optional) From the **Notes** column, click the trash icon to remove a component.

Caution If your vCenter Server instance and all ESXi hosts in the cluster are of version 8.0 Update 3 or later, you can remove the VMware Host Client and ESXi VM Tools components from the base image. To avoid critical errors on any of the hosts in the cluster, make sure you perform thorough testing of the customized image before remediating the cluster.

h (Optional) Click **Hide details** to hide the list of components.

9 (Optional) To validate the image, click the **Validate** button.

You validate an image to check for missing dependencies and component conflicts.

10 Click **Save**.

   Saving the image triggers an automatic compliance check. All hosts in the cluster or the standalone host are checked against the image.

11 In the **Convert to an Image** pane, finish the image setup.

   a Click the **Finish image setup** button.

   b In the **Finish image setup** dialog box, click **Yes, finish image setup**.

Results

You set up an image for the cluster or standalone host. You now manage all hosts in the cluster collectively or the standalone host with a vSphere Lifecycle Manager image for the cluster or host. Upon remediation, the image is installed on all hosts in the cluster or the standalone host.

What to do next

To apply the image to all hosts in the cluster or the standalone host, remediate the cluster or host against the image.

Working with Images

When you manage a cluster or host with a single image, you can change the image at any time. You can edit the image by changing the software that it includes, for example, you can add or remove components, and you can also change the version of the included components. You can also reuse an image by exporting it and importing it into a different cluster or a standalone host.

Using vSphere Lifecycle Manager images starts with setting up an image for a cluster or a host. After you start managing a cluster or a host with a single image, you can edit the image at any time. You can validate the image before saving it to verify that it includes no conflicting components or missing dependencies.

Setting Up an Image for a Cluster or a Host

You can set up an image during the creation of the cluster or when you add a standalone host to a data center or a folder or later. During the creation of a cluster or the addition of a standalone host to a data center or a folder, you can only define the ESXi version and, optionally, a vendor add-on to be included in the image for the cluster or host. You can later edit the image to include additional components or a firmware add-on. For detailed information about creating a cluster and adding hosts to it, and about adding a standalone host to a data center or folder, see the *vCenter Server and Host Management* documentation.

Note When you set up an image, you select an ESXi version and a vendor add-on from the vSphere Lifecycle Manager depot. If no ESXi base images and vendor add-ons are available in the vSphere Lifecycle Manager depot, you must populate the depot with software updates by synchronizing the depot or uploading updates to the depot manually. For detail information about the corresponding procedures, see Synchronize the vSphere Lifecycle Manager Depot and Import Updates to the vSphere Lifecycle Manager Depot.

If you do not set up an image during the creation of the cluster or the addition of the standalone host to a data center or folder, the cluster or the host use baselines, but you can switch to images at any time. When you set up an image during the transition workflow, you can define the full stack of software to run on the hosts in the cluster or on the standalone host. For more information about switching from baselines to images, see Convert a Cluster or a Host That Uses Baselines Into a Cluster or a Host That Uses vSphere Lifecycle Manager Images.

Whereas switching from baselines to images is possible, the reverse operation is not. If a cluster or a host use a single image, regardless of whether you set up the image during the cluster creation or the host addition to the data center or folder, you cannot switch to using baselines for that cluster or standalone host.

Viewing Details About the Image of a Cluster or Host

You can view the software elements that the image for a cluster or host contains on the **Updates** tab for that cluster or host.

The **Image** pane consists of two cards.

The **Image** card contains information about the image that the cluster or host uses. In that card, you perform all image-related operations. You edit the image, you export the image, you validate your selections, and so on. You can also check and view the recommendations that VMware provides.

The **Image Compliance** card contains compliance information about the hosts in the cluster or the standalone host. In that card, you perform host-related operations. You check the compliance of the hosts in the cluster or the standalone host, you run remediation pre-checks, you remediate the hosts in the cluster or the standalone host, and so on.

In the **Image Compliance** card, you edit remediation settings for that cluster or host and manage depot overrides.

Edit a vSphere Lifecycle Manager Image

For a cluster or host that you manage with a single image, you can edit the image at any time to add, remove, or update an image element. For example, you can edit the image to update the vendor add-on version that it includes, to add or remove a driver, to upgrade the ESXi version in the image, and so on.

Working with Image Drafts

When you edit an image, vSphere Lifecycle Manager saves the working copy of the image as a draft. The draft is an edited but unsaved version of an image. If you edit an image but for some reason you do not save the new image set-up, when you restart editing the image, you can use the saved draft version as a starting point or you can altogether discard the changes that you previously made.

Validation

You can validate an image draft before you save it. Validation checks whether the image is correct and complete. During validation, vSphere Lifecycle Manager checks for missing dependencies and conflicting components. In case of issues, vSphere Lifecycle Manager returns messages with information about the existing issues. You must resolve all issues before you can save the image.

Editing an image and validating a draft before saving it are supported operations for clusters with hosts or standalone hosts that have a DPU device. During validation, vSphere Lifecycle Manager validates both the VIBs that are applicable to the ESXi version on the host and to the ESXi version on a DPU device.

Prerequisites

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a cluster or host that you manage with a vSphere Lifecycle Manager image.
2. On the **Updates** tab, select **Hosts > Image**.
3. In the **Image** card, click the **Edit** button.

4 In the **Edit Image** card, modify the image set-up.

Image Element	Possible Modifications
ESXi Version	From the **ESXi Version** drop-down menu, select a new ESXi base image.
Vendor Addon	■ To add a vendor add-on to the image, click **Select** and select a vendor add-on. ■ To change the version of the vendor add-on in the image or to select a new vendor add-on, click the pencil icon and make your changes. ■ To remove the vendor add-on from the image altogether, click the trash icon.
Firmware and Drivers Addon	■ To add a firmware add-on to the image, click **Select**. In the **Select Firmware and Drivers Addon** dialog box, specify a hardware support manager and select a firmware add-on to add to the image. ■ To select a new firmware add-on, click the pencil icon and make your changes. ■ To remove the firmware add-on element from the image altogether, click the trash icon. Selecting a firmware add-on for a family of vendor servers is possible only if the respective vendor-provided hardware support manager is registered as an extension to the vCenter Server where vSphere Lifecycle Manager runs.
Components	Click **Show details** and view the list of additional components in the image. ■ To add components to the image, click **Add Components** and select the components and their corresponding versions to add to the image. **Caution** If your vCenter Server instance and all ESXi hosts in the cluster are of version 8.0 Update 3 or later, you can select and retain a lower version for an additional component that is part of the ESXi base image. To avoid critical errors on any of the hosts in the cluster, make sure you perform thorough testing of the customized image before remediating the cluster. ■ To delete a component from the image, click the trash icon in the table with components. **Caution** If your vCenter Server instance and all ESXi hosts in the cluster are of version 8.0 Update 3 or later, you can remove the VMware Host Client and ESXi VM Tools components from the base image. To avoid critical errors on any of the hosts in the cluster, make sure you perform thorough testing of the customized image before remediating the cluster. ■ To delete a manually added component that overrides a component in the selected vendor add-on or base image, click the undo icon in the table with components. This action reverts the override.

5 (Optional) To validate the image, click the **Validate** button.

You validate an image to check for missing dependencies and component conflicts.

6 Click **Save**.

The save operation triggers validation. If the image is valid, vSphere Lifecycle Manager saves it and runs a compliance check against the new image. You can view compliance information in the **Image Compliance** card.

If the image is invalid, saving the image fails and vSphere Lifecycle Manager returns an error.

Results

The new image is validated and displayed in the **Image** card. vSphere Lifecycle Manager performs an automatic hardware compatibility check against the new image.

If there are recommended images generated for the cluster or host, those recommendations become invalidated and updated. vSphere Lifecycle Manager automatically generates a new recommendation based on the new image.

Export or Import a vSphere Lifecycle Manager Image

You can reuse an image that you already set up for a cluster by exporting it and importing it to another cluster in the same or different vCenter Server instance. Depending on your goal, the image can be exported, distributed, and consumed in three different formats.

You can export the image of a cluster as an ISO image, ZIP file, or a JSON file.

You can import an image to a cluster that uses vSphere Lifecycle Manager images only in the JSON format.

In vSphere 8.0, the export and import operations work for clusters with hosts that have DPU devices.

ISO Image

Distributing an image created with vSphere Lifecycle Manager in an ISO format is useful when you need the image to perform clean installs of ESXi and for bootstrapping purposes, for example the kickstart workflow.

You cannot use an image exported as an ISO file with another cluster that uses vSphere Lifecycle Manager images.

ZIP File

Distributing an image created with vSphere Lifecycle Manager as an offline bundle is useful when you want to import the components that the image contains into the depot of the target vSphere Lifecycle Manager instance.

Unlike the ISO image, you cannot use a ZIP file to create upgrade baselines. You also cannot use the ZIP file to create a vSphere Lifecycle Manager image for a cluster.

JSON File

Distributing an image created with vSphere Lifecycle Manager as a JSON file is useful when you want to reuse the same image for other clusters that use images for host management.

When you distribute the JSON file to clusters in a different vCenter Server instance, you must make sure that the depot of the target vSphere Lifecycle Manager instance contains all components that the JSON file contains.

The JSON file contains only metadata and not the actual software payloads.

Which Distribution Format to Choose?

To reuse an existing image for a cluster in the same vCenter Server system, you must export the image as a JSON file and then import the JSON file to the target cluster.

However, when you want to use an existing image for a cluster in another vCenter Server instance, exporting the image as a JSON file might not be enough. You might also need to export the image as a ZIP file. At the target location, you must import the JSON file as an image to the target cluster. But you might also need to import the ZIP file to the target vSphere Lifecycle Manager depot to make sure that all components included in the image are available to the target vSphere Lifecycle Manager instance.

To reuse an existing cluster image for a cluster that you manage with baselines, you must export the source image as an ISO image. You must then import the ISO image into the local depot of the target vSphere Lifecycle Manager instance and use the imported ISO file to create an upgrade baseline.

Export an Image

You export an image when you want to use the same image for another cluster or standalone host in the same or in a different vCenter Server instance.

Depending on your goals, you can export an image as a JSON file, as an installable ISO image, or as an offline bundle that contains all software packages included in the image. The export format depends on your needs and goals.

For example, if you intend to use the image for a cluster or host in another vCenter Server, you must export it as a JSON file and as a ZIP file. Afterwards, you must import both the JSON file and the ZIP file to the target vCenter Server system. For information about importing updates to the vSphere Lifecycle Manager depot, see Import Updates to the vSphere Lifecycle Manager Depot.

Prerequisites

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or host that you manage with a vSphere Lifecycle Manager image.

2 On the **Updates** tab, select **Hosts > Image**.

3 Click the horizontal ellipsis icon and select **Export**.

4 In the **Export Image** dialog box, select a file format, and click **Export**.

   You can export the image in one file format at a time.

Results

The exported file is saved on your local machine.

What to do next

Import the image to a target cluster or standalone host in the same or in a different vCenter Server instance.

Import an Image

Instead of setting up a new image manually, you can reuse an existing image by importing it to a cluster or a standalone host. Upon remediation, the imported image is applied to all hosts in the cluster or to the standalone host.

You can import an image only if it is in a JSON format. The JSON file contains only the image metadata, but not the actual software payloads. To successfully import an image to a cluster or host and apply the software specification to the hosts in the cluster or to the standalone host, all the components must specified in the image be available in the vSphere Lifecycle Manager depot.

So, if you want to distribute and reuse an image across vCenter Server instances, importing the JSON file might not be enough if the components from the image are not available in the target vSphere Lifecycle Manager depot. In such cases, before you import the JSON file to the target cluster or host, you must first import an offline bundle that contains all components included in the image to the target vSphere Lifecycle Manager depot. If you try to import a JSON file to a cluster or host but the target vSphere Lifecycle Manager depot does not contain the corresponding components, the import operation fails due to validation errors.

For information about importing updates to the vSphere Lifecycle Manager depot, see Import Updates to the vSphere Lifecycle Manager Depot.

Prerequisites

- Verify that the vSphere Lifecycle Manager depot contains all components included in the image that you import.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or host that you manage with a vSphere Lifecycle Manager image.

2 On the **Updates** tab, select **Hosts > Image**.

3 Click the horizontal ellipsis icon and select **Import**.

4 In the **Import Image** dialog box, select a JSON file and click **Next**.

- Enter a URL address to the JSON file that you want to import.
- Browse to a JSON on your local machine.

5 (Optional) In the **Edit Image** card, modify the image set-up.

Image Element	Possible Modifications
ESXi Version	From the **ESXi Version** drop-down menu, select a new ESXi base image.
Vendor Addon	■ To add a vendor add-on to the image, click **Select**. ■ To change the version of the vendor add-on in the image or to select a new vendor add-on, click the pencil icon. ■ To remove the vendor add-on element from the image altogether, click the trash icon .
Firmware and Drivers Addon	■ To add a firmware add-on to the image, click **Select**. ■ To select a new firmware add-on, click the pencil icon. ■ To remove the firmware add-on element from the image altogether, click the trash icon. Selecting a firmware add-on for a family of vendor servers is possible only if the respective vendor-provided hardware support manager is registered as an extension to the vCenter Server where vSphere Lifecycle Manager runs.
Components	Click **Show details** and view the list of additional components in the image. ■ To add components to the image, click **Add Components** and select components to add to the image. ■ To delete a component from the image, click the trash icon in the table with components. ■ To delete a manually added component that overrides a component in the selected vendor add-on, click the undo icon in the table with components. This action reverts the override.

6 If the image contains conflicting components or unresolved dependencies, resolve the issues and retry the procedure.

7 (Optional) To validate the image, click the **Validate** button.

You validate an image to check for missing dependencies and component conflicts.

8 Click **Save**.

A compliance check task is automatically triggered. You can view compliance information in the **Image Compliance** card.

Results

The imported JSON file is imported and set as your new image for the target cluster or host. At that stage, nothing is installed on the hosts in the cluster or on the standalone host. The installation of software on the hosts happens during remediation.

What to do next

Remediate the hosts in the cluster or the standalone host against the new image. See Run a Remediation Pre-Check for a Cluster, a Host Within a Cluster, or a Standalone Host and Remediate a Cluster Against a Single Image.

Check the Compliance Against a Single Image

When you check the compliance of a cluster or host against an image, vSphere Lifecycle Manager compares the software on each host in the cluster or on the standalone host with the software specified in the image. If the image contains a firmware and drivers add-on, the compliance check also calculates the firmware compliance of the hosts with the image. If some of the hosts in the cluster or the standalone host contain DPU devices, vSphere Lifecycle Manager compares the software and firmware on the DPU devices on the hosts with the software and firmware specified in the cluster or host image.

In addition to calculating the compliance state for each host in the cluster or the standalone host, the compliance check gives you information about the impact that the remediate operation will have on a single host, for example if remediation will cause host reboot or if maintenance mode is needed for the host.

A host can have any of the four compliance states: compliant, non-compliant, incompatible, and unknown. If a host has a DPU device, the compliance state of the DPU device is merged into the overall host compliance result.

Compliant

A host is compliant if the image on the host matches the image that you set for the cluster or host.

A DPU-backed host is compliant when the software and firmware on the server and on the DPU device are the same as the software and firmware specified in the image for the cluster or host.

Non-Compliant

A host is non-compliant if the image on the host does not match the image that you set for the cluster or host. A compliant host becomes non-compliant when you set a new image for the cluster or host or manually add or remove components on the host. You remediate non-compliant hosts to make them compliant.

For example, a host is non-compliant in the following cases.

- The ESXi version on the host is earlier than the ESXi version included in the image for the cluster or host.
- The firmware on the host is different from the firmware add-on in the image for the cluster or host.
- The host has a component that is not included in the image for the cluster or host.

- The host contains a standalone VIB.

A DPU-backed host is non-compliant in the following cases:

- ESXi on the server, ESXi on the DPU device, or both have software components of earlier versions than the software and firmware specified in the image for the cluster or host.
- You edit the image for the cluster or host and add a component that contains one or multiple VIBs that are applicable to ESXi on the server, ESXi on the DPU device, or both platforms.
- The remediation of a cluster or a host fails and as a result, the software and firmware components on the host are updated, but the DPU is not updated or the reverse.

Incompatible

A host is incompatible when the image for the cluster or host cannot be applied to the host.

For example, a host is incompatible in the following cases.

- The ESXi version on the host is later than the ESXi version included in the image for the cluster or host.
- The host does not have sufficient resources, for example RAM.
- The hardware of the host is incompatible with the vSphere Lifecycle Manager image for the cluster or host.

A DPU-backed host has the incompatible compliance state when the ESXi version on the DPU is later than the ESXi version included in the image for the cluster or host.

Unknown

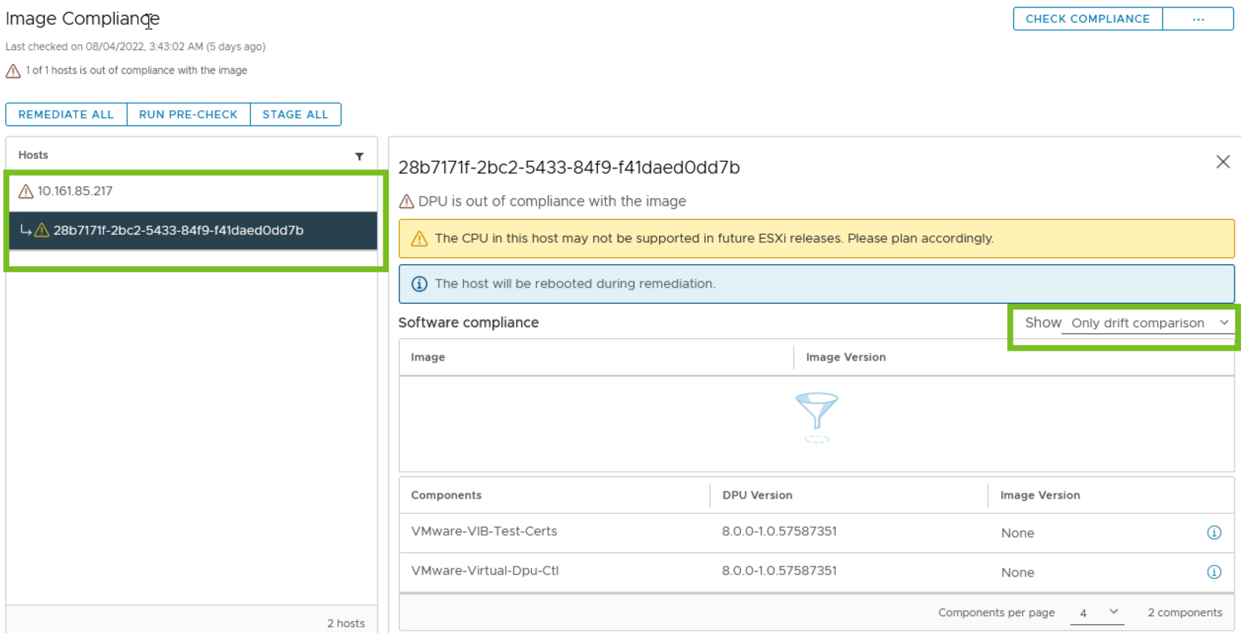
The unknown compliance state indicates that there is no compliance information about the host.

For example, the compliance state of a host is unknown in the following cases.

- You add a new host to the cluster. The compliance state of the newly added hosts is unknown until you perform a compliance check operation on the cluster.
- You add a new standalone host to the data center or folder. The compliance state of the standalone host is unknown until you perform a compliance check operation on the host.
- You edit the image for the cluster or host and save the modifications. The compliance state of all hosts in the cluster or the standalone host is unknown until you check the compliance of the cluster or host against the new image.

Compliance information about the hosts in a cluster or the standalone hosts is displayed on the **Updates** tab for that cluster or host, in the **Image Compliance** card. If you select a cluster, the **Image Compliance** card displays a list of all hosts in the cluster that are out of compliance with the image for the cluster. When you select a host from the cluster, the compliance information about the host appears on the right. If you select a standalone host, the **Image Compliance** card displays the compliance information about the host.

If a host has a DPU device, it is listed directly below the host. The compliance information about the DPU device appears on the right and is presented in an identical manner as the overall compliance information about the host. You can see full image comparison or drift comparison.



Check the Compliance of a Cluster Against a vSphere Lifecycle Manager Image

You check the cluster compliance against an image to understand how each of the hosts in the cluster compares to the specified image.

When you initiate the check compliance operation on an object that contains multiple clusters that you manage with a single image, for example a data center or vCenter Server instance, vSphere Lifecycle Manager performs compliance checks on all those clusters.

Prerequisites

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 In the **Image Compliance** card, click the **Check Compliance** button.

Results

The **Image Compliance** card displays information about the overall number of non-compliant and incompatible hosts in the cluster. You can view detailed compliance information for every host. If the host has a DPU device, you can also view compliance information about the DPU device only.

What to do next

Remediate the cluster to make the non-compliant hosts compliant. See Run a Remediation Pre-Check for a Cluster, a Host Within a Cluster, or a Standalone Host and Remediate a Cluster Against a Single Image.

View Host Compliance Information

You can view detailed compliance information for every non-compliant host in a cluster or for every standalone host that you manage with a single image. You can also view compliance information about the DPU device on the host, if the host has a DPU device. As a result, you can easily find what causes the host to become out of compliance with the cluster or host image.

Detailed compliance information is displayed only for hosts that are out of compliance with the image in the cluster or the standalone host. vSphere Lifecycle Manager displays no compliance details for compliant hosts.

For hosts that have the incompatible compliance state, vSphere Lifecycle Manager shows in a signpost information about what causes the compatibility issues.

Prerequisites

- Run a compliance check.
- Verify that no host is added to the cluster after your last compliance check.

Procedure

1 In the vSphere Client, navigate to a cluster or host that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 View compliance information for the hosts in a cluster or for a standalone host.

Option	Action
View the compliance information for a host in the cluster.	a In the **Image Compliance** card, select a host from the **Hosts** list. **Note** Only non-compliant hosts are listed. b (Optional) To view the full comparison between the image on the host and the image for the cluster, select **Full image comparison** from the drop-down menu for the **Software compliance** table. c (Optional) To view only the image elements that make the host non-compliant with the image for the cluster, select **Only drift comparison** from the drop-down menu for the **Software compliance** table.
View the compliance information for a standalone host.	You can view the compliance information for a standalone host in the **Image Compliance** card. ■ To view the full comparison between the software that runs on the host and the image for the host, select **Full image comparison** from the drop-down menu for the **Software compliance** table. ■ To view only the image elements that make the host non-compliant with the image, select **Only drift comparison** from the drop-down menu for the **Software compliance** table.

4 If you want to view compliance details about a DPU device on a host, select the DPU device listed for the host.

DPU devices are listed directly under the host they belong to.

- To view the full comparison between the image on the DPU device and the image for the cluster or the standalone host, select **Full image comparison** from the drop-down menu for the **Software compliance** table.
- To view only the image elements that make the DPU device non-compliant with the image for the cluster or the standalone host, select **Only drift comparison** from the drop-down menu for the **Software compliance** table.

An information panel appears on the right. In the **Software compliance** table, you can see what software runs on the selected host and what is the software specification in the image for the cluster or the standalone host.

Staging vSphere Lifecycle Manager Images to ESXi Hosts in a Cluster or Standalone Hosts

Staging is the process of downloading depot components from the vSphere Lifecycle Manager depot to the ESXi hosts without applying the software and firmware updates immediately. Staging reduces the time that ESXi hosts spend in maintenance mode.

In vSphere 8.0, staging exists as a separate operation that you can initiate. Staging is also automatically triggered when you remediate a cluster, a host in the cluster, or a standalone host. By default, vSphere Lifecycle Manager performs the staging operation onto all hosts in the cluster in parallel.

If you manage a cluster with a single image, you can stage the image to all hosts in the cluster or to a single host from that cluster. Staging is also supported for clusters with hosts and standalone hosts that have DPU devices. During staging, vSphere Lifecycle Manager downloads to the hosts all components that are applicable to the DPU device.

After staging is successful, a staged icon ( ) appears for any host to which the image is staged. The icon shows that both the software and firmware components from the image are successfully staged to the respective host. If for any reason vSphere Lifecycle Manager can't stage the firmware components to the host, staging does not fail, but you don't see the staged icon for that host.

Staging as Part of Remediation

Starting with vSphere 8.0, the remediation process happens in two steps, staging and then the actual remediation. vSphere Lifecycle Manager puts the ESXi hosts in maintenance mode only after staging is complete. The result is reduced ESXi downtime and disruption in the virtual workloads running on the virtual machines that reside on the respective hosts.

If for some reason staging is successful but the subsequent remediation process fails, the compliance status of the cluster or the standalone host changes from non-compliant to staged.

What Happens With the Staged Content?

The staged content is downloaded to scratch partition if scratch partition has enough space for the staged image. As a result, the staged content is persistent across power-cycles and reboots. If you delete the staged content, vSphere Lifecycle Manager re-stages the components needed for applying the image to the hosts in the cluster or the standalone host as part of the remediation process.

During staging, vSphere Lifecycle Manager validates the checksum and signature of the VIBs and downloads them to the appointed folder only after the validation is successfully completed. When the VIBs become available locally on the hosts, only a root user can modify them.

Staging Firmware Components

If an image contains a drivers and firmware add-on, during staging, the firmware VIBs are staged to the host or hosts along with the other software components defined in the image. If the firmware vendor does not support firmware staging, you get a notification in the **Image Compliance** card. You won't see the staged icon for that host even if staging the rest of the software is successful. In such a case, vSphere Lifecycle Manager installs the firmware components on the hosts during remediation.

Stage an Image to a Cluster

Staging an image to a cluster before remediating the cluster reduces the time that ESXi hosts spend in maintenance mode. After successful staging, you can immediately proceed with remediation, or you can remediate the cluster at a later time.

When you stage an image to a cluster, vSphere Lifecycle Manager downloads all software and firmware components defined in the image from the vSphere Lifecycle Manager depot to all hosts in the cluster. Before you can stage an image to a cluster or a host, you must run a compliance check for the cluster and ensure that the host or hosts to which you stage the image are non-compliant with that image. Staging content to compliant hosts doesn't alter the hosts in any way. Staging the image on hosts whose compliance status is unknown triggers an automatic compliance check.

Prerequisites

- Verify that the hosts in the cluster are non-compliant with the image.
- Verify that the hosts in the cluster are connected to vCenter Server.
- Verify that you have the required privileges to perform the task.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 In the **Image Compliance** card, click the **Stage All** button.

4 (Optional) Click **Skip Remaining Hosts** if you want to stop the staging process while it is ongoing.

   The image is not staged to the skipped hosts.

Results

After staging finishes successfully, an icon ( ) appears for each host for the cluster. The icon shows that all software and firmware from the image are successfully staged to the hosts in the cluster. If for any reason vSphere Lifecycle Manager can't stage the firmware components to the host, staging is still successful, but you don't see the staged icon for the hosts.

What to do next

Remediate the cluster to install the staged software and firmware to the hosts in the cluster.

Stage an Image to a Single Host Within a Cluster or a Standalone Host

Staging is an operation that you can perform for a single host within the cluster or for a standalone host. Learn how to stage an image to a single host from a cluster or to a standalone host.

Prerequisites

- Verify that the hosts in the cluster or the standalone host are non-compliant with the image.
- Verify that the hosts in the cluster or the standalone host are connected to vCenter Server.
- Verify that you have the required privileges to perform the task.

Procedure

1 In the vSphere Client, navigate to a cluster or host that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 Stage a single host.

Option	Action
Stage a single host in a cluster.	a In the **Image Compliance** card, select a host from the **Hosts** list. A card with information about the host appears on the right. b Click **Actions > Stage > .**
Stage a standalone host.	a In the **Image Compliance** card, click the **Stage** button.

Results

After staging finishes successfully, an icon ( ) appears for the host. The icon shows that all software and firmware components from the image are successfully staged to the host. If for any reason vSphere Lifecycle Manager can't stage the firmware components to the host, staging does not fail, but you don't see the staged icon for the host.

What to do next

Remediate the host to install the staged software and firmware components to the host.

Run a Remediation Pre-Check for a Cluster, a Host Within a Cluster, or a Standalone Host

To ensure that the health of a cluster or standalone host is optimal and that no problems occur during remediation, you can perform a remediation pre-check.

The remediation pre-check operation includes a series of checks for the cluster and for each host in the cluster, and for the standalone host. These checks include extensive health checks to determine whether the cluster or host is in a stable state and to ensure successful remediation. Also, the remediation pre-check triggers a compliance check for the cluster or for the standalone host. As a result, after the remediation pre-check, you can view compliance information for each host and whether host reboot or maintenance mode are necessary for successful remediation.

For vSAN clusters, the remediation pre-check operation includes a hardware compatibility check. Depending on how you configure the vSphere Lifecycle Manager remediation settings, vSphere Lifecycle Manager might prevent remediation if hardware compatibility issues exist. For information about configuring the global vSphere Lifecycle Manager remediation settings, see Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image . For information about configuring the remediation settings for a particular cluster, seeOverride the Global vSphere Lifecycle Manager Remediation Settings for a Cluster or Host That You Manage with a Single Image.

Prerequisites

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or host that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 In the **Image Compliance** card, click the **Run pre-check** button.

   You can observe the progress of the pre-check task. When the task finishes, vSphere Lifecycle Manager displays information about the issues found during the pre-check.

What to do next

If vSphere Lifecycle Manager reports no issues, remediate the cluster or the standalone host. See Remediate a Cluster Against a Single Image or Remediate a Single Host Within a Cluster or a Standalone Host Against an Image.

If issues are reported, resolve the issues before you remediate the cluster or the standalone host.

Run a Remediation Pre-Check for a Single Host Within a Cluster or a Standalone Host

Instead of generating a remediation pre-check report for the entire cluster, you can run a remediation pre-check task for a single host in the cluster. You can also run a remediation pre-check for a standalone host in your inventory.

The remediation pre-check task ensures that the host can be successfully remediated.

Prerequisites

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or a standalone host that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 Run a remediation pre-check for the standalone host or a single host within the cluster.

Option	Action
Run a pre-check for a single host within the cluster.	a In the **Image Compliance** card, select a host from the list of hosts. An information panel appears on the right. b Select **Actions > Run pre-check**. The **Running pre-check** card appears above the list of hosts. You can observe the progress of the task.
Run a pre-check for a standalone host.	a In the **Image Compliance** card, click the **Run pre-check** button. The **Running pre-check** dialog appears inside the **Image Compliance** card. You can observe the progress of the task.

Results

When the pre-check finishes, vSphere Lifecycle Manager displays information about the issues found during the pre-check.

What to do next

If vSphere Lifecycle Manager reports no issues, you can remediate the host. See Remediate a Single Host Within a Cluster or a Standalone Host Against an Image.

If vSphere Lifecycle Manager reports any issues, resolve the issues before you remediate the host.

Remediating a Cluster or a Standalone Host Against a Single Image

When you set up or import a vSphere Lifecycle Manager image to use with a cluster or host, the software specified in the image is not immediately installed on the hosts in that cluster or on the standalone host. To apply the software specification from the image to the hosts, you must remediate the cluster or the standalone host against that image.

To initiate remediation of a cluster or host, you must have the required privileges. For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Images. For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation

During remediation, the image that you set up for the cluster is installed on all ESXi hosts in the cluster.

When you remediate a cluster that contains a single ESXi host or that has vSphere DRS deactivated or in manual mode, the remediation process cannot put that host into maintenance mode. So, to proceed with the remediation, you must power off the virtual machines that are running on the host, move them to another host, or select a user policy that allows the remediation process to power off the virtual machines. You can also set a user policy to power on the virtual machines after the host is remediated.

For vSAN clusters, the remediation operation includes a hardware compatibility check. Depending on how you configure the vSphere Lifecycle Manager remediation settings, vSphere Lifecycle Manager might not proceed with the remediation task if hardware compatibility issues exist. For information about configuring the global vSphere Lifecycle Manager remediation settings, see Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image . For information about configuring the remediation settings for a particular cluster or standalone cluster, see Override the Global vSphere Lifecycle Manager Remediation Settings for a Cluster or Host That You Manage with a Single Image.

Maintenance Mode

If the update requires it, hosts are put into maintenance mode before remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure a consistent user experience,vCenter Server migrates the virtual machines to other hosts within the cluster before a host is put into maintenance mode. vCenter Server can migrate the virtual machines if the cluster is configured for vMotion and if DRS and VMware Enhanced vMotion Compatibility (EVC) are enabled. EVC guarantees that the CPUs of the hosts are compatible, but it is not a prerequisite for vMotion.

You can configure vSphere Lifecycle Manager to deactivate HA admission control for the cluster before remediation. However, deactivating HA admission control before you remediate a two-node cluster that uses a single vSphere Lifecycle Manager image causes the cluster to practically lose all its high availability guarantees. The reason is that when one of the two hosts enters maintenance mode, vCenter Server cannot failover virtual machines to that host and HA failovers are never successful. For more information about HA admission control, see the *vSphere Availability* documentation.

Parallel Remediation

During the remediation of a cluster against a vSphere Lifecycle Manager image, the ESXi hosts in the cluster are remediated sequentially by default. So, if the remediation for a single host in the cluster fails, the remediation of the entire cluster stops. However, you can configure vSphere Lifecycle Manager to remediate in parallel the hosts within a cluster that uses images. Parallel remediation reduces the overall remediation time and optimizes the maintenance window for the cluster. You can remediate in parallel only ESXi hosts that are already in maintenance mode. During parallel remediation, hosts do not enter maintenance mode automatically. Similarly, after remediation finishes, the hosts do not exit maintenance mode automatically. To remediate hosts in parallel, you must manually enter and exit maintenance mode. If you activate parallel remediation, vSphere Lifecycle Manager does not remediate the ESXi hosts that are not in maintenance mode.

When you configure vSphere Lifecycle Manager to remediate hosts in parallel, you can set the maximum number of hosts to be remediated in a single remediation task. Alternatively, you can let vSphere Lifecycle Manager calculate the optimal number of hosts to remediate in parallel.

When you remediate hosts in parallel, if the remediation of a single host fails, the remediation task for the entire cluster does not stop and the rest of the hosts are remediated successfully. After remediation finishes, vSphere Lifecycle Manager reports an error for the respective host.

Parallel remediation is deactivated by default, but you can activate it during remediation or in the vSphere Lifecycle Manager general remediation settings. Parallel remediation and all other remediation settings apply to remediation tasks that you start in vCenter Server. Solutions such as NSX, for example, might have separate parallel remediation settings.

You cannot remediate in parallel the witness host and the hosts in the associated vSAN cluster. Parallel remediation is also not possible for clusters that are enabled for vSphere IaaS control plane or NSX.

Remediating a DPU-Backed Cluster or Standalone Host

During remediation, vSphere Lifecycle Manager applies VIBs to the ESXi version on the DPU, if the host has a DPU device and the image for the cluster or host contains components with VIBs applicable to the DPU.

Remediate a Cluster Against a Single Image

By remediating a cluster against an image, you apply the software specified in the image to all the hosts in the cluster. So, by remediating a cluster, you make the non-compliant hosts compliant with the image that you set for the cluster.

During remediation, the hosts in the cluster are remediated in sequence by default. You can configure vSphere Lifecycle Manager to remediate hosts in parallel.

The hosts that have the incompatible compliance state are not remediated.

If a vCenter HA failover is initiated during the remediation of a cluster, the remediation task is canceled. After the failover finishes, you must restart the remediation task on the new node.

Prerequisites

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 In the **Image Compliance** card, click the **Remediate All** button.

   The **Review Remediation Impact** dialog box appears. The dialog box contains detailed information about all changes that remediation will enforce on the hosts in the cluster.

4 In the **Review Remediation Impact** dialog box, review the impact summary, the applicable remediation settings, and the EULA.

5 To save and review the impact details later, click **Export Impact Details**.

6 Accept the EULA by selecting respective check box.

   The check box is selected by default.

7 Click the **Start remediation** button.

   The **Remediate Cluster** task appears in the **Recent Tasks** pane. You can also observe the progress of the remediation task in the **Image Compliance** card. If remediation fails, vSphere Lifecycle Manager gives information about the reasons for the failure.

Remediate a Single Host Within a Cluster or a Standalone Host Against an Image

When you remediate a single host within a cluster or a standalone host against the image for the cluster or host, vSphere Lifecycle Manager applies the image to that host only. Remediation is the operation that makes a non-compliant host in the cluster or a standalone host compliant with the image that you use for that cluster or that host.

Prerequisites

- Verify that the host is non-compliant with the image for the cluster or the standalone host.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a cluster or host that you manage with a single image.
2. On the **Updates** tab, select **Hosts > Image**.
3. Remediate a host within the cluster or a standalone host.

Option	Action
Remediate a single host within a cluster.	a In the **Image Compliance** card, select a host from the **Hosts** list. A card with information about the host appears on the right. b Click **Actions > Remediate >** . The **Review Remediation Impact** dialog box appears. The dialog box contains detailed information about all changes that remediation will enforce on the host.
Remediate a standalone host.	a In the **Image Compliance** card, click the **Remediate** button. The **Review Remediation Impact** dialog box appears. The dialog box contains detailed information about all changes that remediation will enforce on the host.

4. Review the impact summary, the applicable remediation settings, and the EULA.
5. If you remediate a single host in a cluster, to save and review the impact details later, click **Export Impact Details**.
6. Accept the EULA by selecting respective check box.

   The check box is selected by default.
7. Click the **Start remediation** button.

   The **Remediate Cluster** or the **Remediate Host** tasks appear in the **Recent Tasks** pane. You can also observe the progress of the remediation task in the **Image Compliance** card. If remediation fails, vSphere Lifecycle Manager gives information about the reasons for the failure.

View Last Remediation or Remediation Pre-Check Results for a Cluster or a Standalone Host that Uses a Single Image

You can view the remediation results from the last remediation or remediation pre-check that vSphere Lifecycle Manager performed.

Prerequisites

Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or a standalone host that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 In the **Image Compliance** card, click the horizontal ellipsis icon and select your task.

   - To view the results from the last remediation pre-check performed on the cluster or the standalone host, select **Last pre-check results**.
   - To view the results from the last remediation of the cluster or the standalone host, select **Last remediation results**.

Results

The **Image Compliance** displays detailed information about the last remediation or remediation pre-check task that ran on the cluster or the standalone host.

Manage Depot Overrides for a Cluster or a Standalone Host

Instead of accessing the vSphere Lifecycle Manager depot in vCenter Server, clusters or hosts in Remote Office and Branch Office (ROBO) deployments can download data from a depot that is local for them. You can configure vSphere Lifecycle Manager to use local depots for any cluster or standalone host that uses images.

A ROBO cluster or a ROBO standalone host has limited or no access to the Internet or limited connectivity to vCenter Server. As a result, clusters and standalone hosts in ROBO deployments might have limited access to the vSphere Lifecycle Manager depot during the compliance check, remediation pre-check, and remediation operations.

With vSphere Lifecycle Manager images, you can use a local depot for ROBO clusters and hosts, and configure vSphere Lifecycle Manager to use the local depot during the compliance check, remediation pre-check, and the remediation tasks. The local depot overrides the vSphere Lifecycle Manager depot. Using local depots with ROBO clusters and ROBO standalone hosts saves time and network bandwidth.

Starting with vSphere 8.0 Update 1, you can manage local depot overrides for ROBO standalone hosts in the vSphere Client and by using the vSphere Automation API.

For each cluster or standalone host that you manage with a single image, you can add and use multiple local depots instead of the default vSphere Lifecycle Manager depot. You can also delete the depot overrides that you configure. If depot overrides are not active for a cluster or a standalone host, the cluster or the host uses the general vSphere Lifecycle Manager depot in vCenter Server.

Prerequisites

- Set up an online depot to which the cluster or host can connect.
- Export an offline bundle with components from a vSphere Lifecycle Manager image and import the offline bundle to the target local depot.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a cluster or a standalone host that you manage with a single image.
2. On the **Updates** tab, select **Hosts > Image**.
3. In the **Image Compliance** card, click the horizontal ellipsis icon and select **Manage depot overrides**.

   The **Manage depot overrides** dialog box appears.
4. Select your task.

Option	Description
Add depot overrides	Enter a URL or a file path to a local depot and click **Add**. The depot is added to the **Depot override URL** list.
Delete a depot override	Click the horizontal ellipsis icon for a depot override from the list and click **Delete**. The depot is removed from the **Depot override URL** list.

5. Click **Close**.

Results

In the **Image Compliance** pane, you see a notification if depot overrides are active for the cluster or the standalone host.

vSphere Lifecycle Manager Recommended Images

For the clusters that you manage with images, vSphere Lifecycle Manager can generate and provide you with software recommendations in the form of pre-validated images that are compatible with the hardware of the hosts in a cluster. Recommended images are valid images that are based on the latest ESXi version in a series of releases. You can easily replace the current image of a cluster with the recommended image for that cluster.

When you set up or edit an image, you manually combine the image elements (ESXi version, vendor add-on, firmware add-on, and additional components) in such a way as to define the full software stack to run on all hosts in the cluster. You must manually check whether a particular image set-up is complete and valid, and suitable to your environment.

The vSphere Lifecycle Manager recommendations save you the effort of exploring the possible and applicable combinations of image elementsvSphere Lifecycle Manager generates recommendations automatically under certain conditions and upon certain events. Alternatively, you can trigger recommendation generation manually.

Recommended images are validated through a series of checks that ensure that a recommended image has no missing dependencies or conflicting components. For vSAN clusters, the validation also runs a hardware compatibility check against the vSAN Hardware Compatibility List (vSAN HCL). The extensive validation checks ensure that if you decide to use a recommended image for a cluster, the remediation against the recommended image is successful.

To generate recommendations, vSphere Lifecycle Manager checks what software is available in the vSphere Lifecycle Manager depot and what firmware is available in the depot that the selected hardware support manager makes available. Based on the available software, firmware, and, for vSAN clusters, the hardware compatibility checks, for each cluster that you manage with a single image, vSphere Lifecycle Manager provides you with the latest and most appropriate image for your environment.

You can manually cancel the recommendation generation task from the **Recent Tasks** pane.

What Does Latest in Current Series Mean

The recommendation that vSphere Lifecycle Manager generates is based on the major ESXi version in the image that the cluster uses. vSphere Lifecycle Manager recommends the most recent ESXi version that causes no hardware compatibility issues or regressions. The ESXi version in the recommended image is always within the major release series of the ESXi version of the image for the cluster.

The latest image in a series contains the latest minor ESXi version or patch for that version. For example, if the current image for a cluster contains a base ESXi image of version 7.0 and base images of version 7.0 Update 1, 7.0 Update 2, 7.0 Update 3, and 8.0 are available in the vSphere Lifecycle Manager depot, the latest image in the current series recommendation contains ESXi version 7.0 Update 3.

In some cases, the ESXi version in a recommended image might be the same as the ESXi version in the current image for a cluster, but the recommended image might contain a later version of any other image element, for example the vendor add-on, a component, or the firmware add-on.

Why Are Some ESXi Versions not Recommended

The latest ESXi major version available in the depot might not be recommended, because it might be in conflict with upgrade path restrictions or because it causes hardware compatibility issues. Images that are not recommended contain ESXi versions that, if used for a cluster, might lead to regressions.

For example, the current image for a cluster contains a base ESXi image of version 7.0 Update 1 and the vSphere Lifecycle Manager depot contains ESXi images of version 7.0 Update 2, a hot patch for 7.0 Update 2, and 8.0. Upgrading to the ESXi 7.0 Update 2 with the hot patch is an allowed upgrade path. Upgrading further to ESXi 8.0 causes regression, because the recommended image that contains ESXi 8.0 does not contain the hot patch. So, vSphere Lifecycle Manager lists ESXi Update 2 with the hot patch as the latest in current series recommendation. ESXi 8.0 is listed as a not recommended ESXi version.

In some cases, vSphere Lifecycle Manager might list as not recommended an ESXi version within the current release series. The reason is possible hardware compatibility issues.

In the vSphere Client, you can view a list of all ESXi versions that are not recommended for use together with an explanation about the reason why they are not recommended.

Automatically Triggered Recommendation Generation

vSphere Lifecycle Manager generates a new image recommendation automatically in the following cases.

- The vSphere Lifecycle Manager depot gets updated.

  By default, the depot updates every 24 hours. Also, the content of the depot changes when you import an offline bundle to the depot or you manually trigger synchronization to the configurable download sources.

  Note If the depot gets updated with solution components only, vSphere Lifecycle Manager does not generate new recommendations. Similarly, if the depot gets updated by adding or removing base images that are of a major ESXi version as compared to the current image of a cluster, vSphere Lifecycle Manager does not start a recommendation generation task.

- You edit the image that you use for a cluster and save the new image set-up.

  Note If you edit an image by only adding solution components to the image, vSphere Lifecycle Manager generates no new recommendation.

The automated recommendation generation is available only for clusters that already have recommended images generated. When vSphere Lifecycle Manager starts the generation of a new recommendation automatically, the Compute Image recommendations for cluster task appears in the **Recent tasks** pane. You can observe the progress of the task or cancel it. vCenter Server issues an event when a recommendation generation task starts or ends. If the task fails, vCenter Server issues an alarm of the warning type. In cases of failure, you must check for recommended images for the cluster manually. The recommendation generation task cannot run simultaneously with other vSphere Lifecycle Manager operations, for example remediation and compliance checks. If you need to start another operation immediately, you can cancel the Compute Image recommendations for cluster task at any time.

In ROBO deployments, the automatically triggered recommendation generation is possible only if the local depot and the central vSphere Lifecycle Manager depot are synchronized.

Check for Recommended Images

By using recommended images for your clusters or standalone hosts, you ensure that your environment runs the latest verified software. Although vSphere Lifecycle Manager generates image recommendation automatically when the cluster or the host changes or when new software is available in the vSphere Lifecycle Manager depot, you can manually check for recommendations at any time.

A recommended image contains updates for your cluster or host. The recommendations is based on the ESXi versions available in the vSphere Lifecycle Manager depot. When you trigger the **Compute image recommendations** task, vSphere Lifecycle Manager first determines the recommended ESXi version for the cluster or host. After that, vSphere Lifecycle Manager checks sequentially for newer versions of the vendor add-on, additional components, and firmware add-on that are compatible with the recommended ESXi version and the hardware of the hosts in the cluster or the standalone host. So, sometimes, a recommended image might contain the same ESXi version as the ESXi version in the current image for the cluster or host but combined with an updated vendor add-on, component, or firmware add-on.

The **Compute image recommendations** task is non-cancellable. You must rerun the task periodically to ensure that the recommendations are valid and still suitable to the cluster or host.

Before you check for recommended images, you must ensure that the cluster or host is not being remediated. Recommendations generation and remediation are mutually exclusive operations. They cannot run simultaneously.

Prerequisites

- Verify that remediation is not running for the cluster or the standalone host.
- Verify that you have connection to the Internet.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a cluster or a standalone host that you manage with a single image.
2. On the **Updates** tab, select **Hosts > Image**.
3. In the **Image** card, click the horizontal ellipsis icon and select **Check for recommended images**.

   When the task finishes, a blue badge appears in the **Image** card.
4. To view the recommended images, click the horizontal ellipsis icon and select **View recommended images**.

Results

vSphere Lifecycle Manager suggests a recommended image for the cluster or for the standalone host or reports that no recommended images are available for the cluster or the host.

When no recommended images are available, vSphere Lifecycle Manager displays detailed information about why no recommendations are available or why certain ESXi versions are not recommended.

What to do next

View the recommendations. You can import a recommended image to the cluster or host and replace the current image that the cluster or the host uses. See Use the vSphere Lifecycle Manager Recommended Image as the New Image for a Cluster or a Standalone Host.

View the Recommended or Not Recommended Images for a Cluster or a Standalone Host

You can view the pre-validated image that vSphere Lifecycle Manager recommends for a cluster or a standalone host and also the ESXi versions that vSphere Lifecycle Manager does not recommend for that cluster or host because of possible hardware compatibility issues or regression.

Prerequisites

- Verify that the **Compute image recommendations** task is performed for the cluster or the host or check for recommended images for the cluster or the host manually. See Check for Recommended Images.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a cluster or a standalone host that you manage with a single image.
2. On the **Updates** tab, select **Hosts > Image**.
3. If no recommendations are available for the cluster or host at all, click **View Details** in the banner at the top of the pane to see details.
4. If recommendations are available, in the **Image** card, click the horizontal ellipsis icon and select **View recommended images**.
   - To view the image that vSphere Lifecycle Manager recommends for the cluster or the host, check the **Latest in current series** column in the **Recommended Images** dialog box.

- To view the ESXi versions that vSphere Lifecycle Manager doesn't recommend for the cluster or the host, in the **Recommended Images** dialog box, click **Show versions that are not recommended**.

  Note The **Show versions that are not recommended** link is visible only if the vSphere Lifecycle Manager depot contains more recent ESXi versions than the ESXi version in the current cluster or host image, but those more recent versions are not within the major release series of the current base image or might lead to hardware compatibility issues. For example, if the image for your cluster or host contains ESXi version 7.0, and ESXi 8.0 is available in the vSphere Lifecycle Manager depot, the latter is listed as a not recommended version.

If the **View recommended images** option is dimmed, no recommended images are available for this cluster or host. If recommendations are available, in the **Image** card, you see a label indicating the number of recommendations.

The **Recommended Images** dialog box appears.

What to do next

You can decide to use the recommended image and set it as the new image for the cluster or the host.

Use the vSphere Lifecycle Manager Recommended Image as the New Image for a Cluster or a Standalone Host

For any cluster or host that you manage with a single image, you can view the images that vSphere Lifecycle Manager recommends and you can replace the current image for the cluster or the host with a recommended image. Using recommended images saves you the time and effort of identifying valid images that are applicable to all hosts in a cluster or to a standalone host.

Prerequisites

- Check for recommended images for a cluster or a host. See Check for Recommended Images.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or to a standalone host that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 In the **Image** card, click the horizontal ellipsis icon and select **View recommended images**.

   If the **View recommended images** option is dimmed, no recommended images are available for this cluster or host.

   The **Recommended Images** dialog box appears.

4 In the **Recommended Images** dialog box, select a recommended image by clicking the respective radio button and click **Continue**.

   The recommended image is based on the latest ESXi version within the current release series. For example, if the ESXi version in your current image is 7.0, this option might include ESXi version 7.0 Update 3 and a related vendor add-on. The recommended image cannot contain ESXi 8.0 or any other minor release version within the 8.0 release series.

   The selected image is imported to the cluster or the standalone host as a draft. The **Edit Image** card appears.

5 (Optional) Edit the image and validate the new image set-up.

6 Click **Save**.

   If you do not save the image, it is saved as a draft. The next time you start editing the image for that cluster or host, you can use the draft as a starting point.

Results

The recommended image is saved for that cluster or host. If a draft exists for the cluster or the host, the draft is overridden by the recommended image. No software is installed on the hosts in the cluster or on the standalone host at this stage.

What to do next

To apply the software specification that the image defines, remediate the cluster or the host against the new image. See Run a Remediation Pre-Check for a Cluster, a Host Within a Cluster, or a Standalone Host and Remediating a Cluster or a Standalone Host Against a Single Image.

Firmware Updates with vSphere Lifecycle Manager

You can use vSphere Lifecycle Manager images to perform firmware updates on the ESXi hosts in a cluster or on the standalone hosts. With a single operation, you update both the software and the firmware on the host.

In earlier vSphere releases, you could perform firmware updates on vSAN clusters by using system-managed baselines. For non-vSAN clusters, firmware updates had to be manual.

vSphere Lifecycle Manager enables you to easily update the firmware in any cluster or host that you manage with a single image. Firmware updates are not available for clusters or hosts that you manage with baselines.

To apply firmware updates to the hosts in a cluster or to the standalone host that you manage with a single image, you must include a special type of add-on, the firmware and drivers add-on, in the image and remediate the cluster or the host to apply the image to the hosts. The firmware and drivers add-on is a vendor-provided add-on that contains the components that encapsulate firmware update packages. The firmware and drivers add-on might also contain the necessary drivers.

Unlike vendor add-ons, firmware and drivers add-ons are not distributed through the official VMware online depot or as offline bundles available at https://my.vmware.com. For a given hardware vendor, firmware updates are available in a special vendor depot, whose content you access through a software module called a hardware support manager. The hardware support manager is a plug-in that registers itself as a vCenter Server extension. Each hardware vendor provides and manages a separate hardware support manager that integrates with vSphere. For each cluster or host that you manage with a single image, you select the hardware support manager that provides the firmware updates for the cluster or the host. After you determine the hardware support manager that you want to use for a cluster or a standalone host, the hardware support manager provides you with a list of the available firmware updates. When you select and include a firmware add-on to an image, that add-on might modify the specified image by adding or removing components. The firmware add-on also defines the firmware versions to be installed on the hosts. During remediation, vSphere Lifecycle Manager applies the image to the hosts and requests the selected hardware support manager to update the firmware on the hosts in accordance with the firmware add-on specified in the image.

Selecting a hardware support manager and including a firmware add-on in your image guarantees that during a compliance check, vSphere Lifecycle Manager also determines the firmware compliance for the cluster or the host. So, you can easily detect and remediate any unwanted drifts. The hardware support manager is also responsible for retrieving the firmware versions on the host hardware, and, in some cases, determining the appropriate drivers for the updated firmware version.

For vSAN clusters, the hardware support manager inspects the hosts in the cluster to determine their current I/O device controllers and firmware. During a hardware compatibility check for the cluster, vSphere Lifecycle Manager checks whether the firmware in the image is compatible with the hardware in the cluster as per vSAN Hardware Compatibility List (vSAN HCL). The hardware compatibility check ensures that when vSphere Lifecycle Manager remediates the cluster and applies the image to all hosts, the firmware and drivers on the hosts are certified for use with vSAN.

Firmware Updates on DPU Devices

In a DPU-based environment, you can update the firmware on the DPU devices of the hosts through the vSphere Lifecycle Manager remediation operation only if the server vendor has an integrated hardware support manager. For servers that don't provide a hardware support manager, firmware updates are manual.

Deploying Hardware Support Managers

The deployment method and the management of a hardware support manager plug-in are determined by the respective OEM.

Several of the major OEMs develop and supply hardware support managers. For example:

- Dell

The hardware support manager that Dell provides is part of their host management solution, OpenManage Integration for VMware vCenter (OMIVV), which you deploy as an appliance.

- HPE

  The hardware support managers that HPE provides are part of their management tools, iLO Amplifier and OneView, which you deploy as appliances.

- Lenovo

  The hardware support manager that Lenovo provides is part of their server management solution, Lenovo XClarity Integrator for VMware vCenter, which you deploy as an appliance.

- Hitachi

  The hardware support manager that Hitachi provides, Hitachi Unified Compute Platform Advisor, is infrastructure automation and management software for all Hitachi converged, hyperconverged, and integrated systems, which you deploy as an appliance.

- Cisco

  The hardware support manager that Cisco provides is integrated with Cisco Intersight Infrastructure Service, which is part of Cisco Intersight and you activate the hardware support manager from within the Cisco Intersight SaaS-based management platform. No additional appliances are required on your vCenter Server instance.

You can find the full list of all VMware-certified hardware support managers in the VMware Compatibility Guide at https://www.vmware.com/resources/compatibility/search.php?deviceCategory=hsm.

Deploying and Configuring Hardware Support Managers

Regardless of the hardware vendor, you must deploy the hardware support manager appliance on a host with sufficient memory, storage, and processing resources. Typically, hardware support manager appliances are distributed as OVF or OVA templates. You can deploy them on any host in any vCenter Server instance.

Note If vCenter Server is configured with a proxy for internet access, the proxy must be able to reach any hardware support manager registered with that vCenter Server instance. You must either assign the hardware support manager a private IP address within the **10.x.x.x** range, which is automatically exempt from proxy use, or enable a direct access to the registered hardware support manager by configuring the proxy settings with an exception for its IP address.

After you deploy the appliance, you must power on the appliance virtual machine and register the appliance as a vCenter Server extension. You might need to log in to the appliance as an administrator. Each hardware support manager might register with only one or multiple vCenter Server systems.

A vCenter Server plug-in user interface might become available in the vSphere Client after you deploy a hardware support manager appliance, but the hardware support manager might also have a separate user interface of its own. For example, OMIVV, iLO Amplifier, and Lenovo XClarity Integrator for VMware vCenter all have a vCenter Server plug-in user interface, which helps you configure and work with the respective hardware support manager.

Each hardware support manager has its own mechanism of managing the actual firmware packages and making firmware add-ons available for you to choose.

The successful integration between the hardware support manager and vSphere Lifecycle Manager might require a specific configuration of the hardware support manager. For example, with OMIVV, you must first create a connection profile. Then, you must create a cluster profile and associate it with a cluster before you can add a firmware add-on from Dell to the image for that cluster.

With vSphere 8.0 Update 3, vSphere Lifecycle Manager and vSAN integrate to support proactive hardware management. You can deploy and register a hardware support manager that has proactive hardware support management functionality. All hosts in a vSAN cluster associated with such hardware support manager, start receiving proactive notifications about predictive disk failures. You can use these notifications to take early remediation steps before the actual disk failure occurs. Each vendor has a predefined set of health statuses that trigger the respective vCenter Server event. Upon receiving an event regarding disk failure, vSAN raises a health alarm and provides some troubleshooting guidance from the vendor. For more information about proactive hardware management, see the *Managing Proactive Hardware* section in the *vSAN Monitoring and Troubleshooting* documentation. For more information about how to replace failed disks, see the *Replace a Flash Caching Device on a Host in vSAN Cluster* and *Replace a Capacity Device in vSAN Cluster* procedures in the *vSAN Monitoring and Troubleshooting* documentation.

For detailed information about deploying, configuring, and managing hardware support managers, refer to the respective OEM-provided documentation.

Use an Image for Firmware Updates

vSphere Lifecycle Manager allows you to manage the firmware lifecycle on ESXi hosts that are part of a cluster or on a standalone host that you manage with a single image.

Prerequisites

- Deploy the vendor-provided hardware support manager and register it as a vCenter Server extension. For more information about deploying and managing a hardware support manager, see the respective OEM documentation.
- If you use the hardware support manager provided by Dell, create a cluster profile and associate it with the cluster. For more information, review the OpenManage Integration for VMware vCenter (OMIVV) documentation.
- Verify that all hosts in the cluster are from the same vendor.

- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a cluster or a standalone host that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Image**.

3 In the **Image** card, click the **Edit** button.

4 In the **Edit Image** card, for the **Firmware and Drivers Addon**, click **Select**.

   The **Firmware and Drivers Addon** dialog box appears.

5 In the **Firmware and Drivers Addon** dialog box, select a hardware support manager from the drop-down menu.

   The selected hardware support manager must be from the same hardware vendor as the hosts in the cluster or as the standalone host. Otherwise, during a compliance check, the hardware support manager reports the selected firmware and drivers add-on to be incompatible with the host or hosts that are from a different vendor. Firmware remediation fails.

   A list of all available firmware add-ons appears.

6 Select a firmware add-on from the list.

   An information panel appears on the right. The panel contains information about the supported ESXi versions and whether the selected add-on contains the necessary drivers.

7 Click **Select**.

   The selected firmware and drivers add-on is included in the image.

8 In the **Image** card, validate and save the image.

   After the image is saved, a compliance check against the new image is triggered for the cluster or host.

9 In the **Image Compliance** card, review the compliance check results for the cluster and for the host.

10 If any host in the cluster or the standalone host has firmware that is non-compliant with the new image firmware, remediate the respective host or the cluster.

   a (Optional) In the **Image Compliance** card, run a remediation pre-check to ensure that remediation finishes successfully.

      - To run a pre-check for all hosts in the cluster, click the **Run Pre-check** button.
      - To run a pre-check for a single host in the cluster, click the vertical ellipsis icon for the host and select **Run Pre-check**.
      - To run a pre-check for a standalone host, click the **Run Pre-check**.

   b In the **Image Compliance** card, initiate remediation.

      - To remediate all hosts in the cluster, click the **Remediate All** button.

        During cluster remediation, if the remediation of a single host fails, the remediation for the cluster ends prematurely.

      - To remediate a single host, click the vertical ellipsis icon for the host and select **Remediate**.
      - To remediate a standalone host, click the **Remediate** button.

   You are not obliged to start remediation immediately after setting up an image for a cluster or a standalone host. However, nothing is installed on the hosts unless you remediate them against the image for the cluster or the host. The firmware on the hosts is actually updated only after successful remediation. You can remediate the objects in your environment at any time that is convenient for you.

Results

The firmware on the hosts in the cluster or the standalone host is updated to the firmware version specified in the firmware add-on for the image.

vSphere Lifecycle Manager Hardware Compatibility Checks for Clusters and Hosts

7

vSphere Lifecycle Manager automates the process of validating the hardware compliance of hosts and clusters against a selected ESXi version. Hardware compatibility checks ensure that the host or cluster hardware is compliant with the VMware Compatibility Guide (VCG) and vSAN Hardware Compatibility List (vSAN HCL).

Hardware Compatibility Lists

Hardware compatibility lists are lists of hardware certified for use with various vSphere releases. The VCG contains information about server models and I/O devices that are certified for use with particular vSphere releases. Besides VCG, vSAN maintains a separate hardware compatibility list that lists all I/O and networking device controller hardware and the respective firmware versions certified for use with vSAN. The vSAN HCL also contains information about the disk drives that a specific vSphere release supports and the earliest disk drive firmware version certified for use with vSAN.

With vSphere Lifecycle Manager, you can perform the following tasks.

- Check the hardware compatibility of a single host.
- Check the hardware compatibility of a vSAN cluster.

In general, hardware incompatibilities do not prevent remediation and are not resolved upon remediation. However, you can configure vSphere Lifecycle Manager to prevent remediation when hardware compatibility issues exist for a cluster. For information about configuring the global vSphere Lifecycle Manager remediation settings, see Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image . For information about configuring the remediation settings for a particular cluster, see Override the Global vSphere Lifecycle Manager Remediation Settings for a Cluster or Host That You Manage with a Single Image.

Read the following topics next:

Cluster-Level Hardware Compatibility Checks

Running a hardware compatibility check on your clusters before remediating them helps you ensure good vSAN cluster health and avoid entering into unsupported and unwanted configurations after remediation.

Cluster-level hardware compatibility checks are available only for vSAN clusters that you manage with a single image. If a vSAN cluster uses baselines, hardware compatibility checks are not available. Also, if a cluster uses a single vSphere Lifecycle Manager image but vSAN is not enabled for that cluster, hardware compatibility checks for that cluster are not available. Hardware compatibility checks for vSAN clusters are performed against the vSAN HCL.

To perform a hardware compatibility check for a vSAN cluster, the vSAN HCL data that is available to vSphere Lifecycle Manager must be up to date. vSAN HCL data is synchronized automatically or, in environments without connection to the Internet, manually. For more information about maintaining the vSAN HCL data up-to-date, see the vSAN documentation.

When you initiate a hardware compatibility check for a cluster, vSphere Lifecycle Manager scans the image and verifies that all elements of the image are compatible with the hardware of all hosts within the cluster. vSphere Lifecycle Manager validates only those hardware devices that vSAN uses. Because cluster-level hardware compatibility checks validate the compatibility between the cluster hardware and the cluster image, the compatibility results might not be accurate unless you remediate the cluster successfully and apply the image to all hosts in the cluster.

Note vSphere Lifecycle Manager performs the full driver and firmware verification of PCI devices and disk drives only if you configure vSphere Lifecycle Manager with a hardware support manager and add a firmware add-on to the vSphere Lifecycle Manager image. Without using a hardware support manager, vSphere Lifecycle Manager only validates the PCI and NIC devices and their respective driver versions, and the disk drive version.

Hardware compatibility issues are reported as warnings, and as such, they do not prevent you from remediating the hosts in the cluster against the image unless you change that behavior by editing the remediation settings for the cluster. For information about configuring remediation settings for a cluster, see Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image and Override the Global vSphere Lifecycle Manager Remediation Settings for a Cluster or Host That You Manage with a Single Image.

Depending on the type of device, during a hardware compatibility check for a cluster, vSphere Lifecycle Manager performs different validations and verifications during a hardware compatibility check.

Device Type	vSphere Lifecycle Manager Validation
Storage I/O controllers	For storage I/O controllers, vSphere Lifecycle Manager performs the following verifications: ■ Verifies that all storage device controllers are certified for use with the ESXi version specified in the image. ■ Verifies that the image contains the correct storage device driver and firmware versions as per the vSAN HCL. ■ Suggests a compatible storage device driver and firmware version combination as per the vSAN HCL.
Network controllers	For NIC devices, vSphere Lifecycle Manager performs the following verifications: ■ Verifies that the physical RDMA-enabled NICs on the hosts in the cluster are certified for use with the ESXi version specified in the image as per the vSAN HCL. ■ Verifies that the image that the cluster uses contains the correct NIC driver and firmware versions as per the vSAN HCL. ■ Suggests a compatible NIC driver and firmware version combination for the cluster as per the vSAN HCL. ■ Verifies that the device is certified for all active features that are enabled on that device. For example, if vSAN uses a RDMA-capable NIC, vSphere Lifecycle Manager verifies that the NIC is certified for RDMA.
Disk drives	For disk drives, vSphere Lifecycle Manager performs the following verifications: ■ Verifies that all disk drives in the cluster are certified for use with the ESXi version specified in the image as per vSAN HCL. ■ Verifies that the disk drive firmware version specified in the image for the cluster is equal to or higher than the earliest supported firmware version for the device as per vSAN HCL. **Note** vSphere Lifecycle Manager performs those verifications not only on directly connected disk drives, but also on physical disk drives behind RAID-0 logical volumes and behind a VMD controller.

What Are the Currently Active Features

The list of active features for a device is a list of the software features that are enabled on the device and that the device can support. The active features that a device has enabled are the result of enabling or using a solution or a service. In the vSphere Client, information about the currently active features on a device is only available for PCI devices - storage controllers and network controllers. A list of the currently active features is not displayed for disk drives.

When a solution or service, for example vSAN or NSX, enables a set of features on a device, those features impose certain hardware compatibility constraints upon the device. The device must be certified for those active features that vSAN uses. During a hardware compatibility check, in addition to validating the driver and firmware combination for a PCI device, vSphere Lifecycle Manager also validates the constraints that the active features impose on that device. So, by running a hardware compatibility check, you ensure that only certified features are enabled on the devices in the vSAN cluster. You don't get compatibility issues for features that are not enabled on the device.

When the set of active features for a device changes, you must re-run the hardware compatibility check to get correct compliance results.

Hardware Compatibility Check Results

After a hardware compatibility check, vSphere Lifecycle Manager lists a device as compliant or non-compliant. In some cases, the compatibility status is unavailable.

Compliant

A device is compliant when it is compatible with the ESXi version and the driver and firmware version defined in the cluster for the image. For PCI devices, the driver-firmware version combination must also be certified for all active features enabled on the respective device.

Non-compliant

A device is non-compliant when it is incompatible with the ESXi, driver, or firmware version defined in the cluster for the image. Additionally, PCI devices are non-compliant when the driver-firmware version combination is not certified for all active features enabled on the respective device.

If a device is not present in the vSAN HCL at all, vSphere Lifecycle Manager marks the device as non-compliant.

Unavailable

The hardware compatibility status for a NIC device is unavailable in the following cases:

- Compatibility information for PCI devices is unavailable if the vSAN HCL data is not updated and does not contain information about the constraints imposed upon a device by the active features that are enabled on that device.
- The cluster has no hosts or some hosts in the cluster are inaccessible.
- No hardware support manager is registered in vCenter Server or the image for the cluster does not contain a firmware and drivers add-on.

When Does the Hardware Compatibility Check Task Run

vSphere Lifecycle Manager performs regular hardware compatibility checks for the vSAN clusters that you manage with a single image. In addition, certain vSphere Lifecycle Manager operations

also trigger an automatic hardware compatibility check. Automated hardware compatibility checks are available for vSAN clusters that use a single image.

For information about hardware compatibility checks and instructions how to manually perform a hardware compatibility check for a cluster or for a single host, see Chapter 7 vSphere Lifecycle Manager Hardware Compatibility Checks for Clusters and Hosts.

The Hardware Compatibility Check Task

The vSAN Hardware Compatibility List (vSAN HCL) database changes regularly. For example, when VMware certifies new OEM devices, drivers, or firmware, those become part of the vSAN HCL database. Similarly, devices, drivers, or firmware that are not supported anymore are removed from the vSAN HCL database.

Changes in the vSAN HCL database might make your hardware compatibility results invalid and outdated. To provide you with valid hardware compatibility information, vSphere Lifecycle Manager runs a periodic hardware compatibility check against the latest vSAN HCL data.

The periodic hardware compatibility check is a preconfigured scheduled task that you can edit and force to run at any time. By default, the task runs every 24 hours. The scheduled task is configured at a vCenter Server level. If a vCenter Server system contains no vSAN clusters that you manage with a single image, vSphere Lifecycle Manager skips the scheduled hardware compatibility check. This periodic task runs only for vSAN clusters that you manage with a single image.

vSphere Lifecycle Manager Operations That Trigger a Hardware Compatibility Check

vSphere Lifecycle Manager performs an automatic hardware compatibility check for any vSAN cluster that you manage with a single image in the following cases.

- You edit the image for the cluster and save the image.

  When you edit and save an image, vSphere Lifecycle Manager starts the Check hardware compatibility of cluster's host with image task even for clusters without vSAN. In such case, vSphere Lifecycle Manager only returns a warning that image hardware compatibility is not verified in non- vSAN clusters.

  If the automatically triggered hardware compatibility task fails, you can still save the new image for the cluster.

- You initiate a remediation pre-check or remediation.

  The hardware compatibility check is a part of the remediation pre-check and remediation task for vSAN clusters. If a cluster is not vSAN-enabled, vSphere Lifecycle Manager does not perform a hardware compatibility check when you initiate a remediation pre-check or remediation.

You can configure how vSphere Lifecycle Manager behaves in case of hardware compatibility issues by editing the remediation settings for the cluster. For information about configuring remediation settings for a cluster, see Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image and Override the Global vSphere Lifecycle Manager Remediation Settings for a Cluster or Host That You Manage with a Single Image.

- You add or remove a host to and from the cluster.

  When you add or remove a host to and from the cluster, vSphere Lifecycle Manager invalidates the hardware compatibility check results for the cluster and issues a warning. You must rerun a hardware compatibility check to obtain valid information about potential hardware compatibility issues. Alternatively, you can remediate the cluster or run a remediation pre-check, which both automatically trigger a hardware compatibility check.

NIC validation

Starting with vSphere 8.0, hardware compatibility checks for vSAN clusters are enhanced to incorporate NIC validation against the vSAN HCL. Determining the compatibility between the NICs in a vSAN cluster and the software defined in the image that the cluster uses is crucial to a successful cluster upgrade.

During a hardware compatibility check, for each NIC device, vSphere Lifecycle Manager verifies that the driver and firmware version combination defined in the image for the cluster is certified for use with all active features enabled on the device.

For NIC devices, vSphere Lifecycle Manager checks the exact firmware version during the hardware compatibility check.

In a vSAN cluster, during a hardware compatibility check, vSphere Lifecycle Manager validates only the RDMA-capable NICs that vSAN uses. That is, if a host has a RDMA-capable NIC but the NIC is not in use, vSphere Lifecycle Manager does not calculate the hardware compatibility of that device. vSphere Lifecycle Manager does not validate non-RDMA NICs. Non-RDMA NICs in use by vSAN need no certification and therefore vSphere Lifecycle Manager does not validate them during a hardware compatibility check.

System Requirements for NIC Validation

- vCenter Server 8.0 and later
- ESXi 8.0 and later

Disk Drive Validation

During a cluster-level hardware compatibility check, vSphere Lifecycle Manager verifies that the disk drives that vSAN uses are supported and certified as per the vSAN Hardware Compatibility List (vSAN HCL). vSphere Lifecycle Manager also ensures that the disk drive firmware version specified in the cluster image is compatible with the cluster hardware.

The disk drives in a vSAN cluster and the firmware installed on the drives are of paramount importance for the overall vSAN cluster health. For example, a faulty disk drive firmware might cause performance issues and unexpected vSAN input-output behavior. You can use vSphere Lifecycle Manager hardware support managers to perform disk drive firmware upgrades. Before you upgrade the disk drive firmware, however, you must ensure that the target firmware version is supported as per the vSAN HCL.

Note For SAS and SATA disk drives, the vSAN HCL lists the earliest supported firmware version. All firmware versions later than the specified in the vSAN HCL are supported. For NVMe devices behind a VMD controller, the vSAN HCL lists the exact driver-firmware combination certified for use with a given ESXi base image version. Only that specific driver-firmware version combination listed in the vSAN HCL is supported.

Supported Disk Drives Types

vSphere Lifecycle Manager validates the following types of disk drives and storage device configurations:

- HDD (SAS/SATA)
- SSD (SAS/SATA)
- SAS/SATA disk drives behind single-disk RAID-0 logical volumes
- NVMe devices behind a VMD controller

  Note vSphere Lifecycle Manager treats NVMe devices that are not VMD-enabled as PCI storage controllers. In the vSphere Client, hardware compatibility information about NVMe devices that are not VMD-enabled is available on the **PCI Devices** tab and not on the **Disks** tab.

System Requirements for Disk Drive Validation

- vCenter Server 7.0 Update 3 and later
- ESXi 7.0 and later
- For validation of NVMe devices behind a VMD controller, vCenter Server 8.0 and later and ESXi 8.0 and later

  Important Hardware compatibility checks do not validate NVMe devices behind a VMD controller, if the ESXi version of the hosts is earlier than 8.0. If you want to check the hardware compatibility of NVMe devices behind a VMD controller for hosts running an earlier version of ESXi, for example 7.0 Update 3, you have the following workarounds:

  - Override manually the compliance status of the NVMe device behind a VMD controller.
  - Upgrade your hosts to ESXi 8.0 or later.

RAID-0 Logical Volumes

vSphere Lifecycle Manager can validate the physical SAS/SATA disk drives behind single-disk RAID-0 logical volumes. The following requirements exist:

- The RAID controller is in a RAID or mixed mode.

  For more information about the RAID and mixed mode, see the VMware knowledge base article at https://kb.vmware.com/s/article/53573.

- vCenter Server 7.0 Update 3 and later
- ESXi 7.0 and later
- The hardware support manager must be upgraded and certified to work with vSphere 7.0 Update 3.

  If the you do not use an upgraded version of the hardware support manager, the compliance status of the physical drives behind RAID-0 logical volumes is unknown. In this case, you must manually validate the disk drives and the target firmware version and override the compliance status for those disks.

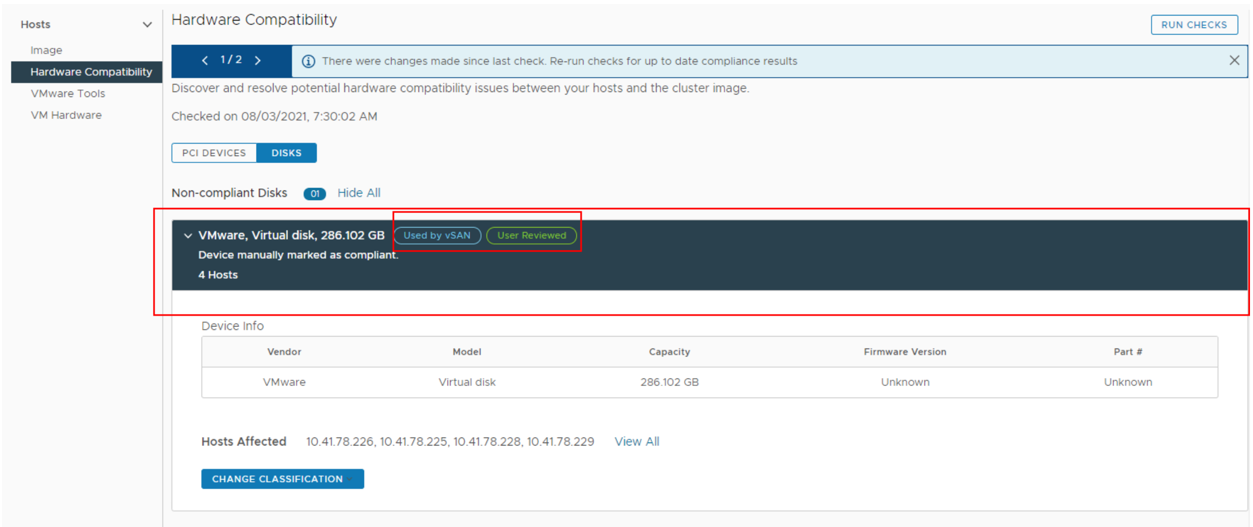
Disk Drive Validation Results

vSphere Lifecycle Manager does not display a disk drive compatibility status and compatibility information for every single disk in the vSAN disk group. vSphere Lifecycle Manager groups the disk drives that vSAN uses by vendor, model, target firmware version, capacity, and part number. That is, all disk drives by the same vendor, the same model, and with the same target firmware version form one entry in the list of disk devices.

Disk drives can be compliant or non-compliant. In the cases when vSphere Lifecycle Manager cannot find a unique match for a disk device in the vSAN HCL, vSphere Lifecycle Manager prompts you to manually specify the exact device that you want to validate. vSphere Lifecycle Manager then calculates the compliance status based on your selection.

When vSphere Lifecycle Manager is unable to determine the disk drive compliance, the respective devices are listed as non-compliant. You can manually validate those devices and set the compliance status to compliant or non-compliant. For more information, see Change the Compliance Status of a Disk Device Manually.

For each entry in the disk device list, you can view summarized information about the disk, the compliance status, the number of affected hosts, and a label that shows whether the compliance status is manually set or whether the device is certified. The **Used by vSAN** label is attached to all disk devices that vSAN uses.



If you expand the entry, you can view detailed compliance information about the respective disk device and the affected hosts.

When a new disk is added to a vSAN cluster, you must manually re-run the check to obtain the new compliance information about the cluster. Similarly, if you remove a disk from the vSAN disk group, you must re-run the hardware compatibility check to obtain an updated compliance information about the cluster.

Check the Hardware Compatibility of a Cluster

For a vSAN cluster that you manage with a single image, you can check the compliance between the image components and the hardware in the cluster. The check is performed against the vSAN Hardware Compatibility List (vSAN HCL) and ensures that if the image is applied to the hosts, the result after remediation is in accordance with the vSAN HCL.

Prerequisites

- Verify that vSAN is enabled for the cluster.
- Verify that the cluster uses a single image.
- Verify that all hosts in the cluster are from the same vendor.
- To validate the compatibility between the PCI device and disk device hardware and target firmware version, verify that the image for the cluster includes a firmware add-on.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a vSAN cluster that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Hardware Compatibility**.

 In the **Hardware Compatibility** pane, you see the results from the previous compatibility check.

3 In the **Hardware Compatibility** pane, click the **Run Checks** button.

Results

vSphere Lifecycle Manager displays all compatibility information and issues in the **Hardware Compatibility** pane. You can see detailed compatibility information for each PCI device or disk drive.

What to do next

Review the result from the hardware compatibility check.

Resolve any issues before you remediate the cluster.

Change the Compliance Status of a Disk Device Manually

You can manually change the compliance status of a disk device and mark it as compliant or non-compliant.

In cases when the compliance status of a disk drive is unavailable, you must perform the hardware compatibility check manually and mark the device as compliant or non-compliant.

Prerequisites

- vCenter Server 7.0 Update 3
- Verify that vSAN is enabled for the cluster.
- Verify that the cluster uses a single image.
- Verify that all hosts in the cluster are from the same vendor.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1 In the vSphere Client, navigate to a vSAN cluster that you manage with a single image.

2 On the **Updates** tab, select **Hosts > Hardware Compatibility**.

 In the **Hardware Compatibility** pane, you see the results from the previous compatibility check.

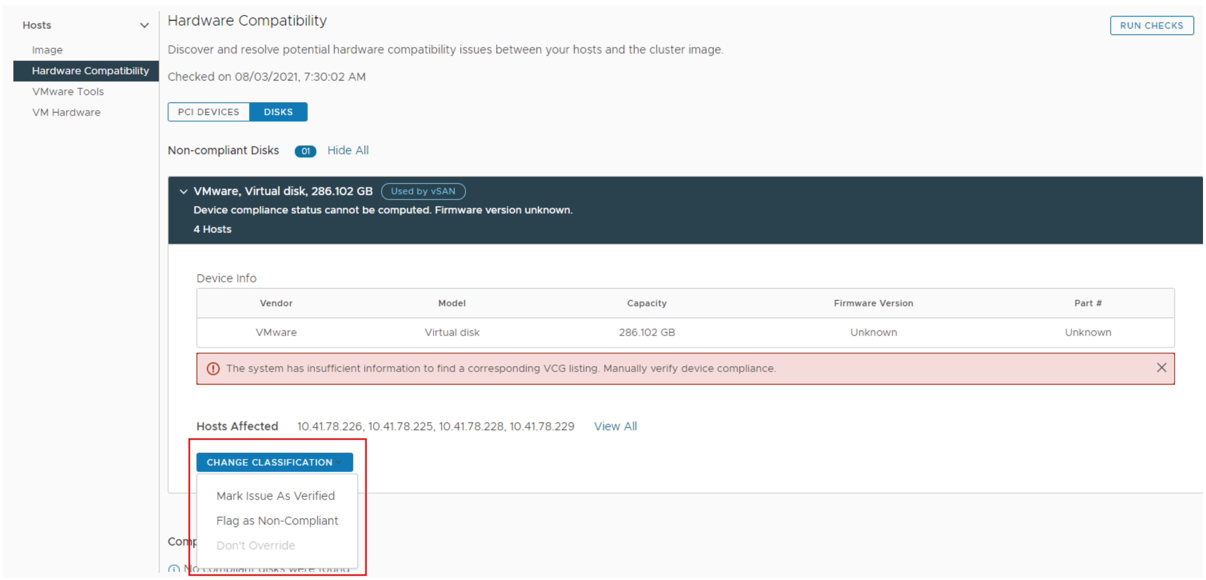
3 Click the **Disks** button.

 You see a list of all non-compliant and compliant disk devices.

4 Click the disk device whose compliance status you want to override.

5 Click the **Change Classification** button.

A drop-down menu appears.



6 Select the compliance status to apply to the disk device.

- To mark the issue as compliant, select **Mark Issue As Verified**.
- To mark the issue as non-compliant, select **Flag as Non-Compliant**.

The **Mark Issue As Verified** option is not available for compliant devices. The **Flag as Non-Compliant** option is unavailable if the disk device is non-compliant

7 (Optional) To undo the override selection, select **Don't Override** from the **Change Classification** drop-down menu.

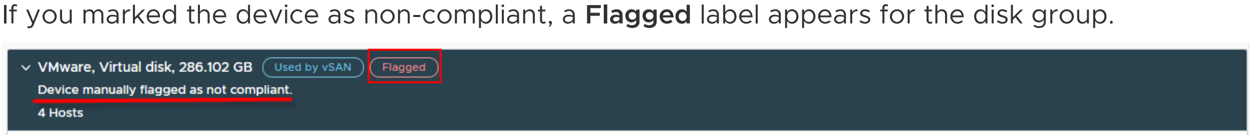
Results

You changed the compliance status of a disk device. However, the disk device remains in its original list until you run a new hardware compatibility check.

If you marked the device as verified, a **User Reviewed** label appears for the disk group.



If you marked the device as non-compliant, a **Flagged** label appears for the disk group.



What to do next

Run a new hardware compatibility check so that the new compliance status for a disk is saved.

Host-Level Hardware Compatibility Checks

You can run a hardware compatibility check for any host to determine which ESXi version the host hardware is compatible with. The hardware compatibility check ensures that the host hardware, that is server model and I/O devices, is certified for use with a selected ESXi version. Host-level hardware compatibility checks are performed against the VMware Compatibility Guide (VCG), even if the host is in a vSAN cluster.

You can check the hardware compatibility of any host, whether it is in a cluster that uses a single image or baselines. You can also check the hardware compatibility of a standalone host. Host-level hardware compatibility checks don't validate the firmware on the host, even if it is part of a cluster that you manage with a single image or if it is a standalone host that you manage with a vSphere Lifecycle Manager image.

After the hardware compatibility check, vSphere Lifecycle Manager shows the compliance status for the server and hardware devices. The server and devices might have one of the three different states: compatible, incompatible, and unknown. For more information about compatibility statuses, see Hardware Compatibility Report for a Host.

If the server status is incompatible, vSphere Lifecycle Manager does not proceed with checking the compatibility for the hardware devices.

Check the Hardware Compatibility of a Host

You can check the hardware compatibility of a host to determine whether the host hardware is certified for use with a selected ESXi version. The hardware compatibility check is performed against the VMware Compatibility Guide (VCG) or, if the host is in a vSAN cluster, against the vSAN Hardware Compatibility List (HCL)

Prerequisites

- If needed, synchronize hardware compatibility data. See Sync Hardware Compatibility Data.
- Verify that the Customer Experience Improvement Program is enabled.
- Verify that vCenter Server is connected to the Internet.
- Verify that the host is not part of an VxRail environment.
- Verify that you have the proper privileges. See vSphere Lifecycle Manager Privileges For Using Images.

Procedure

1. In the vSphere Client, navigate to a standalone host or a host in a cluster.
2. On the **Updates** tab, select **Hosts > Hardware Compatibility**.
3. In the **Hardware Compatibility** pane, select your task.
   - To run a hardware compatibility check for the host for the first time, select a target ESXi from the drop-down menu and click **Apply**.

- To check the hardware compatibility between the host and the already selected target ESXi version, click **Re-run Checks**.
- To choose a new target ESXi version for the hardware compatibility check, click **Edit** and select a new target ESXi version.
- To export the hardware compatibility report in a CSV format, click the **Export** button.

Results

vSphere Lifecycle Manager displays the result from the compatibility check. You can see a list of the compatible, incompatible, and unknown devices. For each device, you can see full details by clicking the expand button.

Hardware Compatibility Report for a Host

The hardware compatibility report gives you information whether for a selected server model and hardware devices, vSphere Lifecycle Manager finds records for a target ESXi version in the VMware Compatibility Guide (VCG).

Server Hardware Compatibility

Host Model is Not Compatible

This compatibility status indicates that there are no records for the selected ESXi version in the VCG. If the host is not compatible with the selected ESXi version, vSphere Lifecycle Manager does not proceed to checking the compatibility of the devices.

In the **Host Model Compatibility** card, you can see details about the host: server model name, CPU model, and the BIOS version running on the host. At the bottom of the card, you see a list of all certified CPU series for the target ESXi version.

Host Model is Compatible

This compatibility status indicates that the host is certified for use with the selected ESXi version as per VCG. When the host is compatible, vSphere Lifecycle Manager proceeds with the device validation.

In the **Host Model Compatibility** card, you can see details about the host: server model name, CPU model, and the BIOS version running on the host. Because in VCG the information about CPUs is based on CPU series, and not specific models, you might need to manually check if the CPU of the host is part of the supported CPU series. You might also need to manually check if the BIOS version on the host matches any of the compatible BIOS versions for the CPU series as per VCG.

Hardware Compatibility Checks Not Supported for the Host Vendor Model

When the server model is not part of the list of certified OEMs, vSphere Lifecycle Manager does not perform a hardware compatibility check and you do not see a hardware compatibility report for the selected host.

Device Hardware Compatibility

The compatibility statuses for devices are: compatible, incompatible, and unknown.

Unknown

Unknown devices are devices for which no records exist in VCG. When you click the expand button for the device, you see the following device information: device IDs, driver and firmware currently running on the device. No compatibility data is generated and displayed.

The unknown status might also indicate that multiple matches exist in the VCG for the respective device. In such cases, use the device ID to manually check if the hardware device matches any of the supported devices for the target ESXi version in the VCG.

Incompatible

The incompatible status indicates that no records exist in the VCG for the selected ESXi version. When you click the expand button for the device, you see information about the ESXi versions that are compatible with the device as per VCG.

Compatible

The compatible status indicates that the device is compatible with the selected ESXi version as per VCG. When you click the expand button for the device, you see the following device information: device IDs, driver and firmware currently running on the device. For compatible devices, you might need to manually confirm that the driver-firmware combination running on the device is supported as per VCG.

Sync Hardware Compatibility Data

To initiate a hardware compatibility check for a host, the hardware compatibility data from VMware Compatibility Guide (VCG) must become available to vSphere Lifecycle Manager.

Synchronizing compatibility ensures that the compatibility information from VCG becomes available to vSphere Lifecycle Manager. The synchronization task is not automated. When no compatibility data is available for use to vSphere Lifecycle Manager, you must trigger the compatibility data synchronization manually.

vSAN HCL data is not updated through synchronization. If you want to check the hardware compatibility of a host that is in a vSAN cluster, you must first verify that vSAN HCL data is up to date. For more information about updating vSAN HCL data, see the vSAN documentation.

Prerequisites

Verify that vCenter Server can access the following sites:

- vvs.esp.vmware.com
- auth.esp.vmware.com

Procedure

1 In the vSphere Client, navigate to a standalone host or a host in a cluster.

2 On the **Updates** tab, select **Hosts > Hardware Compatibility**.

3 In the **Hardware Compatibility** pane, click **Sync compatibility data**.

4 In the **Sync hardware compatibility data** dialog box, click **Go to Lifecycle Manager**.

   You are redirected to the vSphere Lifecycle Manager home view.

5 Select **Actions > Sync HCL**.

   The Update HCL data task appears in the **Recent Taks** pane.

Results

After the Update HCL data task finishes, the compatibility data from the VCG becomes available to vSphere Lifecycle Manager.

What to do next

Check the hardware compatibility of your hosts against VCG before you update or upgrade them to a later ESXi version.

Using vSphere Lifecycle Manager Baselines and Baseline Groups

8

Using baselines and baseline groups to manage the updates and upgrades of ESXi hosts is a multi-stage process.

1 Populate the vSphere Lifecycle Manager repository with patches, extensions, and updates.

   The vSphere Lifecycle Manager repository contains software updates that you can use with both vSphere Lifecycle Manager baselines and vSphere Lifecycle Manager images. On the

   Updates tab of the vSphere Lifecycle Manager home view, you see all software updates available in the vSphere Lifecycle Manager depot as bulletins.

   Updates get into the vSphere Lifecycle Manager local depot through synchronization with configurable download sources. By default, vSphere Lifecycle Manager is configured to synchronize updates from the official VMware depot.

   You can also import updates into the depot manually.

   For host upgrade operations through baselines, you use ESXi ISO images, which you must also import to the vSphere Lifecycle Manager depot manually.

   For more information about working with the vSphere Lifecycle Manager depot, see Chapter 2 The vSphere Lifecycle Manager Depot.

2 Create baselines by combining bulletins from the depot and using manually uploaded ESXi ISO images.

   You can also combine several non-conflicting baselines to create a baseline group. Baseline groups can contain different types of baselines. If a baseline group contains both upgrade and patch or extension baselines, the upgrade runs first.

   For more information about creating baselines and baseline groups, see Types of vSphere Lifecycle Manager Baselines and Baseline Groups.

3 Attach the baselines to individual ESXi hosts or container objects for ESXi hosts.

   For more information, see Attach Baselines and Baseline Groups to Objects.

4 Check the compliance of ESXi hosts against a selected baseline or baseline group.

   You can run a compliance check on an individual ESXi host or a container object.

   For more information about compliance checks against baselines and baseline groups, see Checking Compliance Against vSphere Lifecycle Manager Baselines and Baseline Groups.

5 Review the compliance status of the scanned object.

For more information about compliance states, see Viewing Compliance Information About ESXi Hosts and Updates.

6 Optionally, you can stage the patches and extensions to ESXi hosts before remediation. Staging is not a mandatory step, it is a step that you can skip.

For more information about staging updates before remediation, see Stage Patches and Extensions to ESXi Hosts.

7 Remediate the non-compliant objects. After remediation, you can review the compliance status again to make sure that the updates are installed.

For more information about remediating objects against baselines and baseline groups, see Remediating ESXi Hosts Against vSphere Lifecycle Manager Baselines and Baseline Groups .

Read the following topics next:

- Types of vSphere Lifecycle Manager Baselines and Baseline Groups
- Create, Edit, or Delete vSphere Lifecycle Manager Baselines and Baseline Groups
- Attach Baselines and Baseline Groups to Objects
- Checking Compliance Against vSphere Lifecycle Manager Baselines and Baseline Groups
- Viewing Compliance Information About ESXi Hosts and Updates
- Stage Patches and Extensions to ESXi Hosts
- Remediating ESXi Hosts Against vSphere Lifecycle Manager Baselines and Baseline Groups
- Using vSphere Lifecycle Manager to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch

Types of vSphere Lifecycle Manager Baselines and Baseline Groups

You use baselines and baseline groups to update the ESXi hosts in your vSphere inventory. The vSphere Lifecycle Manager baselines are three types: predefined baselines, recommendation baselines, or custom baselines, which you create manually. Depending on their content, baselines can be patch, extension, or upgrade baselines.

When you initiate a compliance check for an ESXi host, you evaluate it against baselines and baseline groups to determine its level of compliance to those baselines or baseline groups.

If your vCenter Server system is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, the baselines and baseline groups that you create and manage are applicable only to the inventory objects managed by the vCenter Server system where the selected vSphere Lifecycle Manager instance runs.

In the vSphere Client, the baselines and baseline groups are displayed on the **Baselines** tab of the vSphere Lifecycle Manager home view.

Predefined, Recommendation, and Custom Baselines

Predefined baselines

Predefined baselines cannot be edited or deleted, you can only attach or detach them to inventory objects.

Predefined baselines can be of the following type:

- Host Security Patches

  The Host Security Patches baseline checks ESXi hosts for compliance with all security patches.

- Critical Host Patches

  The Critical Host Patches baseline checks ESXi hosts for compliance with all critical patches.

- Non-Critical Host Patches

  The Non-Critical Host Patches baseline checks ESXi hosts for compliance with all optional patches.

The Host Security Patches, and Critical Host Patches predefined baselines are attached by default to the vCenter Server instance where vSphere Lifecycle Manager runs.

Recommendation Baselines

Recommendation baselines are predefined baselines that vSAN generates.

You use recommendation baselines to update your vSAN clusters with recommended critical patches, drivers, updates, or the latest supported ESXi host version for vSAN.

These baselines appear by default when you use vSAN clusters with ESXi hosts of version 6.0 Update 2 and later in your vSphere inventory. If your vSphere environment does not contain any vSAN clusters, no recommendation baselines are created.

Recommendation baselines update their content periodically, which requires vSphere Lifecycle Manager to have constant access to the Internet. The vSAN recommendation baselines are typically refreshed every 24 hours.

Recommendation baselines cannot be edited or deleted. You do not attach recommendation baselines to inventory objects in your vSphere environment. You can create a baseline group by combining multiple recommendation baselines, but you cannot add any other type of baseline to that group. Similarly, you cannot add a recommendation baseline to a baseline group that contains upgrade, patch, and extension baselines.

Custom Baselines

Custom baselines are the baselines that you create. You can create custom patch, extension, and upgrade baselines to meet the needs of your specific deployment.

Upgrade, Patch, and Extension Baselines

Upgrade Baselines

Host upgrade baselines define the version to which you upgrade the hosts in your environment. With vSphere Lifecycle Manager 8.0, you can upgrade ESXi hosts from version 6.7 and 7.0 to ESXi 8.0. Host upgrades to ESXi 5.x, ESXi 6.7, or ESXi 7.0 are not supported. In case of an unsuccessful upgrade from ESXi 6.7 or ESXi 7.0 to ESXi 8.0, you cannot roll back to your previous ESXi 6.7 or ESXi 7.0 instance.

To create an upgrade baseline, you must first import an ESXi ISO image to the vCenter Server inventory. You can use the ESXi installer image distributed by VMware with the name format `VMware-VMvisor-Installer-8.0-`*`build_number`*`.x86_64.iso` or a custom image created by using vSphere ESXi Image Builder. You can also use ISO images created and distributed by OEMs.

Patch Baselines

Patch baselines define a number of patches that must be applied to a given host. Patch baselines can be either dynamic or fixed.

Baseline	Description
Dynamic Patch Baseline	A dynamic baseline is a set of patches that meet certain criteria. You specify the criteria for patch inclusion in the baseline. Only the patches that meet the criteria are included in the baseline. As the set of available patches in the vSphere Lifecycle Manager depot changes, dynamic baselines are updated as well. You can manually include or exclude patches from the baseline.
Fixed Patch Baseline	A fixed baseline is a set of patches that does not change as patch availability in the depot changes. You manually select the patches from the total set of patches available in the vSphere Lifecycle Manager depot.

Extension Baselines

Extension baselines contain additional software modules for ESXi hosts, for example device drivers. This additional software might be VMware software or third-party software. All third-party software for ESXi hosts is classified as host extension, but extensions are not restricted to just third-party software.You can install additional modules by using extension baselines, and update the installed modules by using patch baselines.

Extensions deliver additional host features, updated drivers for hardware, Common Information Model (CIM) providers for managing third-party modules on the host, improvements to the performance or usability of the existing host features, and so on.

The host extension baselines that you create are always fixed. You must carefully select the appropriate extensions for the ESXi hosts in your environment.

You use extension baselines to install extensions on the ESXi hosts in your environment. After an extension is installed on a host, you can update the extension module through either patch, or extension baselines.

Note When you use extension baselines, you must be aware of the functional implications that the installation of new modules on the host might have. Extension modules might alter the behavior of ESXihosts. During the installation of extensions, vSphere Lifecycle Manager only performs the checks and verifications expressed at the package level.

Baseline Groups

You create a baseline group by assembling existing and non-conflicting baselines. Baseline groups allow you to scan and remediate objects against multiple baselines at the same time.

The following are valid combinations of baselines that can make up a baseline group:

- Multiple host patch and extension baselines.
- One upgrade baseline, multiple patch, and extension baselines.

To create, edit, or delete baselines and baseline groups, you must have the **Manage Baseline** privilege. To attach baselines and baseline groups to target inventory objects, you must have the **Attach Baseline** privilege. The privileges must be assigned on the vCenter Server system where vSphere Lifecycle Manager runs.

For more information about managing users, groups, roles, and permissions, see the *vSphere Security vSphere Security* documentation.

For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.

Creating Baselines in vSphere 7.0 and Later Releases

Because in vSphere 7.0 and later releases the official VMware online depot hosts certified partner content in addition to VMware content, a broader set of OEM bulletins are available in the vSphere Lifecycle Manager depot. As a result, in the **Create Baseline** and **Edit Baseline** wizards, you also see a broader set of OEM bulletins. Some of these bulletins might have dependencies that must be pulled into the baselines that you create, so that the remediation against those baselines is successful. Always consult the KB article for an individual bulletin before you include it in a baseline. The KB article contains information about the bulletin deployment specifics and required dependencies. You must include in the baseline, only bulletins compatible with the hardware on which the host is running. Otherwise, remediation might fail.

Starting with vSphere 7.0, some changes are also introduced in the way VMware content is packaged. As a result, at patch and update releases, you might see additional bulletins on the patch selection page of the **Create Baseline** and **Edit Baseline** wizards. Those bulletins are usually of the Enhancement or BugFix category. When you include those bulletins in a baseline, you might need to also include base ESXi bulletins in that baseline. To ensure successful application of VMware patches and updates, always include the appropriate roll-up bulletin into your baselines. Otherwise, remediation might fail.

Create, Edit, or Delete vSphere Lifecycle Manager Baselines and Baseline Groups

You can create upgrade baselines for ESXi hosts with ESXi 8.0 images, which you must first import to the vSphere Lifecycle Manager depot.

Prerequisites

- Required privileges: **VMware vSphere Lifecycle Manager.Manage Baselines**.
- To create an upgrade baseline, verify that you have an ESXi 8.0 image available in inventory. For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.

Procedure

1 In the vSphere Client, click the bars icon and select **Lifecycle Manager**.

2 (Optional) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

3 On the **Baselines** tab, select **New > Baseline**.

   If you want to create an upgrade baseline, you can start the **Create Baseline** wizard from the **Imported ISOs** tab. Select an ESXi image from the list and click **New Baseline**.

4 On the **Name and Description** page, enter information about the baseline, select the baseline type and click **Next**.

5 Follow the prompts to finish creating the baseline.

Baseline Type	Steps
Patch Baseline	To create a fixed patch baseline, perform the following steps: a On the **Select Patches Automatically** page, stop the automatic updates by deselecting the respective check box and click **Next**. b On the **Select Patches Manually** page, select the patches that you want to include in the baseline and click **Next**. ■ To view only the rollup bulletins in the list, turn on the **Show only rollup updates** toggle switch. ■ To filter the patches that are available in the vSphere Lifecycle Manager depot and find specific patches to include in the baseline, use the filter icon next to each column header. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND. c On the **Summary** page, review your selections and click **Finish**. To create a dynamic patch baseline, perform the following steps: a On the **Select Patches Automatically** page, set the criteria for adding patches to the baseline. 1 Enable the automatic update of the baseline by selecting the respective check box. 2 On the **Criteria** tab, specify the criteria that a patch must meet to be added to the baseline and click **Next**. **Note** The relationship between the selected criteria is defined by the Boolean operator AND. For example, when you select a product and severity option, the patches are restricted to the ones that are applicable for the selected product and are of the specified severity level. ■ **Patch Vendor** specifies which patch vendor to use. **Note** In vSphere 7.0 and later releases, the vendor name of VMware for inbox components is changed from VMware, Inc to VMware. As a result, if you use the filter to see only components by VMware, the filtered list contains both VMware, Inc for 6.x patches and VMware for 7.x and 8.x patches. ■ **Product** restricts the set of patches to the selected products or operating systems. **Note** The asterisk at the end of a product name is a wildcard character for any version number. ■ **Severity** specifies the severity of patches to include. ■ **Category** specifies the category of patches to include. ■ **Release Date** specifies the range for the release dates of the patches. 3 (Optional) On the **Matched** tab, deselect patches from the ones that matched your criteria to exclude them permanently from the baseline. 4 (Optional) On the **Excluded** and **Selected** tabs, view the patches that are excluded from the baseline and the ones that are included in the baseline.

Baseline Type	Steps
	You can use the filter icon next to each column header on the **Matched**, **Excluded**, and **Selected** tabs to filter the patches that are available in the vSphere Lifecycle Manager depot. This way, you can easily find specific patches to exclude from or include in the baseline. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND. b On the **Select Patches Manually** page, select individual patches to include in the baseline and click **Next**. The patches that are displayed on this page are patches that do not meet the criteria you set on the **Select Patches Automatically** page. You can use the filter icon next to each column header to filter the patches that are available in the vSphere Lifecycle Manager depot and find specific patches to include in the baseline. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND. The patches that you add manually to the dynamic baseline stay in the baseline regardless of the automatically downloaded patches. c On the **Summary** page, review your selections and click **Finish**.
Upgrade Baseline	a On the **Select ISO** page, select an ESXi image from the list and click **Next**. b On the **Summary** page, review your selections and click **Finish**.
Extension Baseline	a On the **Select Extensions** page, select individual extensions to include in the baseline and click **Next**. You can use the filter icon next to each column header to filter the extensions that are available in the vSphere Lifecycle Manager depot and find specific extensions to include in the baseline. If you use several criteria to filter the patches, the relationship between those filter criteria is defined by the Boolean operator AND. b On the **Summary** page, review your selections and click **Finish**.

Results

The new baseline appears in the baselines list on the **Baselines** tab.You can attach the baseline to a data center, a cluster, or a host.

Create a Host Baseline Group

You can combine multiple baselines of different types into a baseline group. For example, you can combine one host upgrade baseline with multiple patch or extension baselines, or you can combine multiple patch and extension baselines.

A baseline group might contain a single host upgrade baseline and multiple patch or extension baselines, or a combination of host patch and host extension baselines.

You can create a baseline group and add baselines to it later.

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Manage Baselines**

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Baselines** tab, select **New > Baseline Group**.

   The **Create Baseline Group** wizard opens.

3 On the **Name and Description** page, enter a unique name and, optionally, a description for the baseline group, and click **Next**.

4 (Optional) On the **Upgrade Baseline** page, select an upgrade baseline to include in the baseline group and click **Next** .

   a Select the **Add the following Upgrade Baseline to the Group** check box.

   b Select an upgrade baseline from the list.

5 (Optional) On the **Patch Baselines** page, select patch baselines to include in the baseline group and click **Next**.

6 (Optional) On the **Extension Baselines** page, select extension baselines to include in the baseline group and click **Next**.

7 On the **Summary** page, review your selections and click **Finish**.

Results

The new host baseline group appears in the baselines list on the **Baselines** tab. You can attach the baseline group to a data center, a cluster, or a host.

Edit a vSphere Lifecycle Manager Baseline or Baseline Group

You can edit existing patch, upgrade, or extension baselines.

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Manage Baselines**

Procedure

1 In the vSphere Client, click the bars icon and select **Lifecycle Manager**.

2 (Optional) Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

3 On the **Baselines** tab, select a baseline or a baseline group from the list and click **Edit**.

The **Edit Baseline** or **Edit Baseline Group** wizard appears.

4 Follow the prompts to finish editing the selected baseline or baseline group.

What to do next

Attach the edited baseline or baseline group to a data center, a cluster, or a host.

Add or Remove a Single Update from a Custom Baseline

You can edit the content of a custom baseline by adding or removing individual patches or extension from the baseline.

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Manage Baselines**

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 Click the **Updates** tab.

You see a list of all updates in the vSphere Lifecycle Manager depot.

3 Select a patch or extension from the list, and click **Add/Remove Baselines**.

The **Add/Remove baselines** dialog box opens.

4 Select your task.

- To add the patch to a baseline, select that baseline in the **Custom Patch Baselines** list.
- To remove the patch from a baseline, deselect that baseline in the **Custom Patch Baselines** list.

5 Click **OK**.

Delete Baselines and Baseline Groups

You can delete the baselines and baseline groups that you no longer need. Deleting a baseline detaches it from all the objects to which it is attached. You cannot delete predefined and system-managed baselines.

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager.Manage Baselines**

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

      The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Baselines** tab, select a baseline or a baseline group from the list and click **Delete**.

   The **Delete Baseline** dialog box opens.

3 Click **Yes** to confirm the deletion of the selected baseline or baseline group.

Attach Baselines and Baseline Groups to Objects

To check the compliance status of the objects in your inventory against selected baselines and baseline groups, you must first attach the respective baselines and baseline groups to the objects.

You attach baselines and baseline groups to individual hosts or objects that contain hosts, such as clusters, data centers, and vCenter Server instances. In the vSphere infrastructure hierarchy, the baseline and baseline groups that you attach to container objects are also attached to the child objects. For example, if you attach a baseline or baseline group to a folder, the baseline or the baseline groups is inherited by all the objects in the folder, including subfolders.

You cannot use vSphere Lifecycle Manager to update the hosts in a cluster that uses a single vSphere Lifecycle Manager image. For more information about using vSphere Lifecycle Manager images to manage hosts in clusters collectively, see Chapter 6 How to Use vSphere Lifecycle Manager Images .

Prerequisites

- If you want to attach a baseline or a baseline group to a cluster, verify that the cluster is not configured to use a single image.
- Required privileges: **VMware vSphere Lifecycle Manager.Manage Baselines.Attach Baseline**.

Procedure

1 In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.

   a Navigate to a host, cluster, or a container object.

   b Click the **Updates** tab.

2 Select **Hosts > Baselines**.

3 In the **Attached Baselines** pane, click **Attach > Attach Baseline or Baseline Group**.

   The **Attach** dialog box opens.

4 Select one or more baselines or baseline groups and click **Attach**.

   If you select a baseline group, all the baselines in it are attached to the object.

   The selected baselines or baseline groups are attached to the object. They appear on the list in the **Attached Baselines** pane. If the selected object is a container object, the selected baselines or baseline groups are attached to all the child objects.

What to do next

Scan the selected object against the attached baselines.

Detach Baselines and Baseline Groups from Objects

You can detach baselines and baseline groups from the objects to which the baselines or baseline groups are directly attached.

vSphere inventory objects might have inherited properties, so instead of detaching baselines and baseline groups directly from an object, you might need to select its container object and detach the baselines or baseline groups from the container object. For example, if you want to detach a baseline or a baseline group from a host that is a part of a cluster, you must select the cluster and not the host.

Prerequisites

- Verify that the cluster is not configured to manage all its hosts collectively.
- Required privileges: **VMware vSphere Lifecycle Manager.Manage Baselines.Attach Baseline**.

Procedure

1 In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.

   a Navigate to a host, cluster, or a container object.

   b Click the **Updates** tab.

2 Select **Hosts > Baselines**.

3 In the **Attached Baselines** pane, select one or more baselines or baseline groups and click **Detach**.

   The **Detach** dialog box opens.

4 Select the object to detach the baseline or baseline group from and click **Detach**.

   The baseline is removed from the **Attached Baselines** list.

Checking Compliance Against vSphere Lifecycle Manager Baselines and Baseline Groups

Before you update or upgrade an ESXi host or a container object with vSphere Lifecycle Manager baselines, you must first check its compliance status.

You use vSphere Lifecycle Manager to check the compliance status of ESXi hosts against the baselines and baseline groups that you attach to the hosts or to a parent container object. You do a compliance check on hosts to determine whether they have the latest patches or extensions. During the compliance check, attributes of the host are evaluated against all patches, extensions, and upgrades from an attached baseline or baseline group.

You can check the compliance status of a single ESXi host or a valid container object. Supported groups of ESXi hosts include virtual infrastructure container objects such as folders, clusters, and data centers. When you initiate a compliance check for a container object, vSphere Lifecycle Manager scans all the ESXi hosts in that container object.

Note If you initiate a compliance check for an inventory object, for example data center, that contains clusters that use vSphere Lifecycle Manager images, the compliance check is not performed for those clusters.

To generate compliance information, you can initiate compliance checks manually or you can schedule the compliance checks to run at regular periods. Schedule compliance checks at a data center or vCenter Server system level to make sure that the objects in your inventory are up-to-date.

You check the compliance status of vSphere objects from the vSphere Lifecycle Manager compliance view.

To initiate or schedule compliance checks, you must have the **Scan for Applicable Patches, Extensions, and Upgrades** privilege.

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.

Initiate a Compliance Check for ESXi Hosts Manually

Before remediation, you must check the compliance of the vSphere objects against the attached baselines and baseline groups. To check the compliance status of hosts in the vSphere inventory immediately, initiate a compliance check manually.

Prerequisites

If you want to check the compliance status of a cluster, verify that the cluster is not configured to use a single image.

Procedure

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
    a. Navigate to a host, cluster, or a container object.
    b. Click the **Updates** tab.
2. Select **Hosts > Baselines**.

    The **Baselines** pane shows three panels. In those panels, you obtain host information about the selected object, host compliance information, and remediation information.
3. In the compliance information panel, click **Check Compliance**.

Results

The selected inventory object and all child objects are scanned against all attached patch, extension, and upgrade baselines. The larger the virtual infrastructure and the higher up in the object hierarchy that you initiate the scan, the longer the scan takes.

Schedule Regular Compliance Checks for ESXi Hosts

You can configure vSphere Lifecycle Manager to check the compliance status of ESXi hosts at specific times or at intervals that are convenient for you.

Prerequisites

If you want to check the compliance status of a cluster, verify that the cluster is not configured to use a single image.

Procedure

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
    a. Navigate to a host, cluster, or a container object.
    b. Click the **Updates** tab.

2 Select **Hosts > Baselines**.

   The **Baselines** pane shows three panels. In those panels, you obtain host information about the selected object, host compliance information, and remediation information.

3 In the compliance information panel, click **Schedule**.

   The **Automatic compliance check** dialog box opens.

4 Configure the compliance check schedule.

   a Set the frequency and the starting point of the compliance check.

   b Enter a unique name, and optionally, a description for the scan task.

   c (Optional) Specify one or more email addresses to receive notification after the scan task is complete.

      You must configure mail settings for the vCenter Server system to enable this option.

5 Click **Save** to exit the **Automatic compliance check** dialog box.

View Information About the Patches, Extensions, and ISO Images in a Baseline

You can view information about the patches, extensions, and upgrades included in a baseline or a baseline group.

For information about the different compliance statuses that an update might have, see Compliance Statuses of Updates.

Prerequisites

- Verify that the host for which you want to view compliance information uses baselines and is not managed with a single vSphere Lifecycle Manager image.
- Review the The vSphere Lifecycle Manager Compliance View topic.

Procedure

1 In the vSphere Client, navigate to a single ESXi host, cluster, or a valid container object.

2 On the **Updates** tab, select **Hosts > Baselines**.

3 In the **Attached Baselines and Baseline Groups** pane, select a baseline.

   A new pane appears below the **Attached Baselines and Baseline Groups** pane. Depending on the selected object, the bottom pane might contain information about the updates and ESXi images in the baseline that you select. If the selected object is a container for ESXi hosts, the bottom pane shows the compliance of each ESXi in the container object against the selected baseline.

Baseline Type	Available Information
Patch	The bottom pane contains a table that lists all patches in the baseline. For each update, you can see the following information. ■ **Update Name** ■ **Update ID** The update ID is a vendor-assigned identification code of the patch. ■ **Status** The **Status** column shows the compliance status of the update. ■ **Severity** ■ **Category** ■ **Impact** The **Impact** column displays the actions that you must take to install the update. For example, rebooting the system or putting the host in maintenance mode. ■ **ESXi Version**
Upgrade	The bottom pane displays the following information. ■ **ESXi Version** ■ **Build** ■ **Status** The **Status** column shows the compliance status of the update. ■ **Release Date** ■ **Vendor** ■ **Details** ■ **Release Notes** ■ **Acceptance Level** ESXi images can be either Signed or Unsigned, which indicates their level of acceptance by VMware. The software packages included in ESXi images might have any of the following acceptance levels. **VMware Certified** The package has gone through a rigorous certification program that verifies the functionality of the feature, and is signed by VMware with a private key. VMware provides customer support for these packages. **VMware Accepted**

Baseline Type	Available Information
	The package has gone through a less rigorous acceptance test program that only verifies that the package does not destabilize the system, and is signed by VMware with a private key. The test regimen does not validate the proper functioning of the feature. VMware support hands off support calls directly to the partner. **Partner Supported** The partner has signed an agreement with VMware and has demonstrated a sound test methodology. VMware provides a signed private/public key pair to the partner to use for self-signing their packages. The VMware support team redirects support calls directly to the partner. **Community Supported** The package is either unsigned or signed by a key that is not cross-signed by VMware. VMware does not provide support for the package. For support, customers must either use the community or contact the author of the package.
Extension	■ **Update Name** ■ **Update ID** The update ID is a vendor-assigned identification code of the extension. ■ **Status** The **Status** column shows the compliance status of the update. ■ **Severity** ■ **Category** ■ **Impact** The **Impact** column displays the actions that you must take to install the update. For example, rebooting the system or putting the host in maintenance mode. ■ **ESXi Version**
Baseline Group	To view information about the patches, extension, and ISO images in a baseline group, select the respective tab in the bottom pane. ■ Click **Baselines** for information about the baselines that a baseline group contains. ■ Click **ISO** for information about the ESXi image that a baseline group contains. ■ Click **Updates** for information about the patches and extensions that the baseline group contains.

Host Upgrade Compliance Messages

When you check the compliance of ESXi hosts against an upgrade baseline, vSphere Lifecycle Manager runs a precheck script and provides informative messages in the in the bottom pane of the vSphere Lifecycle Manager compliance view. The messages notify you about potential problems with hardware or third-party software on the host, and configuration issues, which might prevent a successful upgrade to ESXi 8.0.

The messages that vSphere Lifecycle Manager provides correspond to error or warning codes from running the host upgrade precheck script.

For interactive installations and upgrades performed by using the ESXi installer, the errors or warnings from the precheck script are displayed on the final panel of the installer, where you are asked to confirm or cancel the installation or upgrade. For scripted installations and upgrades, the errors or warnings are written to the installation log.

vSphere Lifecycle Manager displays scan result information in the bottom pane of the vSphere Lifecycle Manager compliance view. To see the original errors and warnings returned by the precheck script during an vSphere Lifecycle Manager host upgrade scan operation, review the vSphere Lifecycle Manager log file.

Table 8-1. Scan Result Messages and Corresponding Error and Warning Codes

Scan Result Message invSphere Lifecycle Manager	Description
`Host CPU is unsupported. New ESXi version requires a 64-bit CPU with support for LAHF/SAHF instructions in long mode.`	This message appears if the host processor is 32-bit and does not support required features. The corresponding error code is `64BIT_LONGMODESTATUS`.
`Trusted boot is enabled on the host but the upgrade does not contain the software package esx-tboot. Upgrading the host will remove the trusted boot feature.`	This message indicates that the host upgrade scan did not locate the `esx-tboot` VIB on the upgrade ISO. The corresponding error code is `TBOOT_REQUIRED`
`VMkernel and Service Console network interfaces are sharing the same subnet` *`subnet_name`*`. This configuration is not supported after upgrade. Only one interface should connect to subnet` *`subnet_name`*`.`	Warning. An IPv4 address was found on an enabled Service Console virtual NIC for which there is no corresponding address in the same subnet in the vmkernel. A separate warning appears for each such occurrence. The corresponding error code is `COS_NETWORKING`.
`New ESXi version requires a minimum of` *`core_count`* `processor cores.`	The host must have at least two cores. The corresponding error code is `CPU_CORES`.
`Processor does not support hardware virtualization or it is disabled in BIOS. Virtual machine performance may be slow.`	Host performance might be impaired if the host processor does not support hardware virtualization or if hardware virtualization is not turned on in the host BIOS. Enable hardware virtualization in the host machine boot options. See your hardware vendor's documentation. The corresponding error code is `HARDWARE_VIRTUALIZATION`.

Table 8-1. Scan Result Messages and Corresponding Error and Warning Codes (continued)

Scan Result Message invSphere Lifecycle Manager	Description
`Insufficient memory, minimum` *`size_in_MB`* `required for upgrade.`	The host requires the specified amount of memory to upgrade. The corresponding error code is `MEMORY_SIZE`.
`Host upgrade validity checks for` *`file_name`* `are not successful.`	This test checks whether the precheck script itself can be run. The corresponding error code is `PRECHECK_INITIALIZE`.
`The host partition layout is not suitable for upgrade.`	Upgrade is possible only if there is at most one VMFS partition on the disk that is being upgraded and the VMFS partition starts after sector 1843200. The corresponding error code is `PARTITION_LAYOUT`.
`Unsupported configuration.`	The file `/etc/vmware/esx.conf` must exist on the host. This message indicates that the file /etc/vmware/esx.conf is either missing, or the file data cannot be retrieved or read correctly. The corresponding error code is `SANE_ESX_CONF`.
`The host does not have sufficient free space on a local VMFS datastore to back up current host configuration. A minimum of` *`size_in_MB`* `is required.`	The host disk must have enough free space to store the ESXi 5.x configuration between reboots. The corresponding error code is `SPACE_AVAIL_CONFIG`.
`The upgrade is not supported for current host version.`	Upgrading to ESXi 8.0 is possible only from ESXi 6.7 and ESXi 7.0 hosts. The corresponding error code is `SUPPORTED_ESX_VERSION`.
`Unsupported devices` *`device_name`* `found on the host.`	The script checks for unsupported devices. Some PCI devices are not supported with ESXi 8.0. The corresponding error code is `UNSUPPORTED_DEVICES`.
`Host software configuration requires a reboot. Reboot the host and try upgrade again.`	To ensure a good bootbank for the upgrade, you must reboot the hosts before remediation. The corresponding error code is `UPDATE_PENDING`.

Table 8-1. Scan Result Messages and Corresponding Error and Warning Codes (continued)

Scan Result Message invSphere Lifecycle Manager	Description
In an environment with Cisco Nexus 1000V Distributed Virtual Switch, vSphere Lifecycle Manager displays different messages in different situations. For details, see Host Upgrade Compliance Messages When Cisco Nexus 1000V Is Present.	If Cisco's Virtual Ethernet Module (VEM) software is found on the host, the precheck script checks if the software is part of the upgrade as well, and that the VEM supports the same version of the Virtual Supervisor Module (VSM) as the existing version on the host. If the software is missing or is compatible with a different version of the VSM, the script returns a warning and the scan result indicates the version of the VEM software that was expected on the upgrade ISO, and the version, if any, that was found on the ISO. The corresponding error code is `DISTRIBUTED_VIRTUAL_SWITCH`.
`The host uses an EMC PowerPath multipathing module` *`file_name`* `to access storage. The host will not be able to access such storage after upgrade.`	The script checks for installation of EMC PowerPath software, consisting of a CIM module and a kernel module. If either of these components is found on the host, the script verifies that matching components (CIM, VMkernel module) also exist in the upgrade. If they do not, the script returns a warning that indicates which PowerPath components were expected on the upgrade ISO and which, if any, were found. The corresponding error code is `POWERPATH`.

Host Upgrade Compliance Messages When Cisco Nexus 1000V Is Present

When a host is managed by the Cisco Nexus 1000V virtual switch and you check the compliance of the host against an upgrade baseline, the scan messages provide information about problems with compliance between the VEM modules installed on the host and the modules available on the ESXi 8.0 image.

vSphere Lifecycle Manager supports Cisco Nexus 1000V, a virtual access software switch that works with VMware vSphere and consists of two components.

Virtual Supervisor Module (VSM)

The control plane of the switch and a virtual machine that runs NX-OS.

Virtual Ethernet Module (VEM)

A virtual line card embedded in ESXi hosts.

vSphere Lifecycle Manager determines whether a host is managed by Cisco Nexus 1000V. vSphere Lifecycle Manager verifies whether the Cisco Nexus 1000V VEM VIBs in the ESXi upgrade image are compatible with the Cisco Nexus 1000V VSM that manages the host.

By using vSphere ESXi Image Builder, you can create custom ESXi images, which contain third-party VIBs that are required for a successful remediation operation.

Table 8-2. Compliance Check Results for the Cisco Nexus 1000V Network Switch

Compliance Check Message	Description
`The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V software package on the host. Upgrading the host will remove the feature from the host.`	A VEM VIB is not available on the ESXi 8.0 upgrade image.
`The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade contains a Cisco Nexus 1000V software package` *`VIB_name`* `that is incompatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.`	The VEM VIB on the ESXi 8.0 upgrade image is not compatible with the version of the VSM.
`The host is currently added to a Cisco Nexus 1000V virtual network switch. The upgrade does not contain any Cisco Nexus 1000V software package that is compatible with the Cisco Nexus 1000V VSM. Upgrading the host will remove the feature from the host.`	The host and the image do not contain VEM VIBs, but the host is still listed in vCenter Server as managed by Cisco Nexus 1000V.
`Cannot determine whether the upgrade breaks Cisco Nexus 1000V virtual network switch feature on the host. If the host does not have the feature, you can ignore this warning.`	There was a problem with determining compatibility between the VEM VIB on the ESXi 8.0 upgrade image and the VSM. Check whether the version of the VSM managing the host is certified as being compatible with vCenter Server 8.0 and ESXi 8.0.

Viewing Compliance Information About ESXi Hosts and Updates

vSphere Lifecycle Manager scans objects to determine how they comply with the baselines and baseline groups that you attach to those objects. You can view compliance information about a single ESXi host or a group of hosts in a container object.

Supported groups of ESXi hosts include virtual infrastructure container objects such as folders, clusters, and data centers.

The host or the container object must have an attached baseline or baseline group to be examined for compliance information. Compliance with baselines and baseline groups is assessed at the time of viewing.

The overall compliance status of an ESXi hosts depends on the compliance statuses of all baselines and baseline groups that are attached to the object. For information about the different compliance statuses that an object, a baseline or a baseline group might have, see Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups .

The compliance status of a baseline depends on the compliance statuses of all updates in the baseline. For information about the compliance statuses that updates might have, see Compliance Statuses of Updates.

The ability to view the compliance status of vSphere objects depends on the privileges that you have. To view the compliance status of an inventory object, you must have the **View Compliance Status** privilege. Users that have privileges to remediate against patches, extensions, and upgrades and to stage patches and extensions on a particular inventory object, can view the compliance status of the same object even if they do not have the **View Compliance Status** privilege.

- Users with the privilege to view a container, but not all the contents of the container, can view the aggregate compliance status of all objects in the container.
- If a user does not have the permission to view an object, its contents, or a particular virtual machine, the results of those scans are not displayed.

For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.

For information about checking the compliance of hosts against an image, see Check the Compliance of a Cluster Against a vSphere Lifecycle Manager Image.

The vSphere Lifecycle Manager Compliance View

Compliance information about inventory objects is displayed on the **Updates** tab for the object, in the so-called vSphere Lifecycle Manager compliance view.

The vSphere Lifecycle Manager compliance view for objects that you manage with baselines and baseline groups consists of three panes.

Table 8-3. vSphere Lifecycle Manager Compliance View

Pane	Description
Baselines	The **Baselines** pane has three information panels. ■ Host Information panel For individual ESXi hosts, this panel shows information about the ESXi version installed on the host. You can also view all updates that are installed on the host. For container objects, this panel shows information about the ESXi versions of all hosts in the container object. ■ Compliance Information panel For individual ESXi hosts, this panel shows the overall compliance status of the host against all attached baselines and baseline groups. You can also view compliance information about the baselines and baseline groups attached to the host. For container objects, this panel shows the overall number of compliant and non-compliant hosts. This panel also shows the last time a compliance check was completed. ■ Remediation Information panel This panel shows the result of the remediation pre-check and indicates whether the selected object is ready for remediation. The panel also contains information about the issues that require user attention or action. This panel also shows the last time a remediation pre-check was completed. The information in the **Baselines** pane changes dynamically depending on the inventory object, baselines, and baseline groups that you select.
Attached Baselines and Baseline Groups	Displays the baselines and baseline groups attached to the selected object.
Bottom pane	The bottom pane appears when you select a baseline or a baseline group from the **Attached Baselines and Baseline Groups** pane. The information in this pane depends on the type of inventory object that you select. For individual hosts, the bottom pane shows information about all updates in the baseline or baseline group that you select from the **Attached Baselines and Baseline Groups** pane. ■ If you select a patch baseline or extension baseline, the bottom pane shows a list of all updates that the selected baseline contains. ■ If you select an upgrade baseline, the bottom pane shows information about the ESXi image that the upgrade baseline contains. ■ If you select a baseline group, the bottom pane shows all baselines included in the group along with their compliance statuses. You can also view all the updates that the baseline group contains. If the baseline group contains an ESXi image, information about it is also displayed in the bottom pane.

Table 8-3. vSphere Lifecycle Manager Compliance View (continued)

Pane	Description
	For container objects, the bottom pane displays compliance information about the ESXi hosts that have the selected baseline or baseline group. When you select a baseline or a baseline group from the **Attached Baselines and Baseline Groups** pane, the bottom pane appears and displays all the hosts to which the selected baseline or baseline group is attached along with the individual compliance statuses of those hosts.

Compliance Statuses of Updates

When you work with vSphere Lifecycle Manager baselines, an update stands for all patches, extensions, and upgrades that you can apply with vSphere Lifecycle Manager baselines. The compliance status of the updates in the baselines and baseline groups that you attach to objects in your inventory is calculated after you check the compliance of the target object.

The compliance statuses of the updates in a baseline define the overall compliance status of that baseline. For more information about baseline compliance statuses, see Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups .

Conflict

The update conflicts with either an existing update on the host or another update in the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform compliance checks, remediation, and staging operations. In most cases, you must resolve the conflict.

Conflicting New Module

The host update is a new module that provides software for the first time, but it is in conflict with either an existing update on the host or another update in the vSphere Lifecycle Manager depot. vSphere Lifecycle Manager reports the type of conflict. A conflict does not indicate any problem on the target object. It just means that the current baseline selection is in conflict. You can perform scan, remediation, and staging operations. In most cases, you must resolve the conflict.

Incompatible Hardware

The hardware of the selected object is incompatible or has insufficient resources to support the update. For example, when you perform a host upgrade scan against a 32-bit host or if a host has insufficient RAM.

Installed

The update is installed on the target object and no further user action is required.

Missing

The update is applicable to the target object, but it is not yet installed. You must perform a remediation on the target object with this update, so that the update becomes compliant.

Missing Package

The metadata for the update is in the depot, but the corresponding binary payload is missing. The reasons can be that the product might not have an update for a given locale; the vSphere Lifecycle Manager depot is corrupt, and vSphere Lifecycle Manager no longer has Internet access to download updates; or you have manually deleted an upgrade package from the vSphere Lifecycle Manager depot.

New Module

The update is a new module. An update with this compliance status cannot be installed when it is part of a host patch baseline. When it is part of a host extension baseline, the new module status indicates that the module is missing on the host and can be provisioned by remediation. The compliance status of the baseline depends on the type of baseline containing the update with the New Module status. If the baseline is a host patch baseline, the overall status of the baseline is compliant. If the baseline is a host extension baseline, the overall status of the baseline is non-compliant.

Not Applicable

The update is not applicable to the target object. A patch might have the not applicable compliance status for one of the following reasons:

- There are other patches in the vSphere Lifecycle Manager depot that obsolete this patch.
- The update does not apply to the target object.

Not Installable

The update cannot be installed. The compliance check might succeed, but the remediation of the target object cannot be performed.

Obsoleted By Host

This compliance status is mainly applicable to patches. The target object has a newer version of the patch. For example, if a patch has multiple versions, after you apply the latest version to the host, the earlier versions of the patch have the Obsoleted By Host compliance status.

Staged

This compliance status applies to host patches and host extensions. It indicates that the update is copied from the vSphere Lifecycle Manager depot to the host, but it is not yet installed. Staged compliance status might occur only when you check the compliance status of hosts running ESXi6.7 and later.

Unknown

A patch is in the unknown state for a target object until vSphere Lifecycle Manager successfully scans the object. A scan might not succeed if the target object is of an

unsupported version, if vSphere Lifecycle Manager lacks metadata, or if the patch metadata is corrupt.

Unsupported Upgrade

The upgrade path is not supported. For example, the current hardware version of the virtual machine is later than the latest version supported by the host.

Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups

Compliance statuses are computed after you initiate a compliance check for an inventory object against the attached baselines or baseline groups. The compliance statuses that baselines and baseline groups might have depend on the applicability of the patches, extensions, and upgrades contained in the baseline or baseline group attached to an object. The compliance status of a single host depends on the compliance statuses of all baselines and baseline groups attached to the host.

Compliant

The compliant status indicates that a vSphere object is compliant with all baselines in an attached baseline group or with all patches, extensions, and upgrades in an attached baseline. The compliant state requires no further action. If a baseline contains patches or upgrades that are not relevant to the target object, the individual updates, and baselines or baseline groups that contain them, are treated as not applicable, and represented as compliant. Compliant are also hosts with attached patch baselines containing extensions or patches with the obsoleted by host status.

The compliant status occurs under the following conditions:

- Target objects are compliant with the baselines and baseline groups when all updates in the baseline or baseline group are either installed on the target object, obsoleted by host, or are not applicable to the target object.
- The updates in a baseline are compliant when they are installed on the target object, or are not applicable to the object.

Non-Compliant

The non-compliant status indicates that one or more baselines in a baseline group, or one or more patches, extensions, or upgrades in a baseline are applicable to the target object, but are not installed (missing) on the target. You must remediate the target object to make it compliant.

When a baseline contains a non-compliant update, the overall status of the baseline is non-compliant. When a baseline group contains a non-compliant baseline, the overall status of the baseline group is non-compliant. The non-compliant status takes precedence over the incompatible, unknown, and compliant states.

Unknown

When you attach a baseline or a baseline group to a vSphere object and you do not initiate a compliance check for the object, the status of the vSphere object against the baseline or baseline group is unknown. This status indicates that a compliance check is required, that the compliance check has failed, or that you initiated a compliance check on an unsupported platform.

When a baseline contains updates in the compliant and unknown states, the overall status of the baseline is unknown. When a baseline group contains unknown baselines and compliant baselines, the overall status of the baseline group is unknown. The unknown compliance status takes precedence over the compliant status.

Incompatible

The incompatible status requires attention and further action. You must determine the reason for incompatibility by probing further. You can remediate the objects that have this status, but the operation might not be successful. In most cases,vSphere Lifecycle Manager provides sufficient details for the incompatibility.

When a baseline contains updates in the incompatible, compliant, and unknown states, the overall status of the baseline is incompatible. When a baseline group contains incompatible, unknown, and compliant baselines, the overall status of the baseline group is incompatible. The incompatible compliance status takes precedence over the compliant and unknown compliance statuses.

View Compliance Information About ESXi Hosts

You can check how the ESXi hosts in your environment comply with the baselines and baseline groups that you attach to those hosts. You can check and view the compliance status of an individual host or a container object.

Compliance checks provide information about the degree of compliance of an object with the attached baselines and baseline groups.

In the compliance view for an object, you can view information about the compliance of the object with the attached baselines and baselines groups. You can also view the individual compliance statuses of the attached baselines and baseline groups. The compliance view changes dynamically and depends on the object that you want to view compliance information about. For a full description of the compliance information that you can obtain about an object, seeThe vSphere Lifecycle Manager Compliance View.

For information about the different compliance statuses that an object might have, see Compliance Statuses of ESXi Hosts, Baselines, and Baseline Groups .

Prerequisites

- Verify that the host for which you want to view compliance information uses baselines and is not managed with a single vSphere Lifecycle Manager image.
- Review the The vSphere Lifecycle Manager Compliance View topic.

Procedure

1 In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.

   a Navigate to a host, cluster, or a container object.

   b Click the **Updates** tab.

2 Select **Hosts > Baselines** and review the compliance information in the compliance view.

Results

You see complete compliance information about the selected object.

Stage Patches and Extensions to ESXi Hosts

Staging is the process during which vSphere Lifecycle Manager downloads patches and extensions on the ESXi hosts. During staging, the patches and extensions are not installed on the host. Staging reduces the time that the host spends in maintenance mode during remediation.

To stage patches or extensions to hosts, first attach a patch or extension baseline or a baseline group containing patches and extensions to the host. Staging patches and extensions does not require that hosts enter maintenance mode.

With the vSphere Client, you can stage a single baseline, multiple baselines, or baseline groups to a single host or a group of hosts in a container object.

Some limitations exist depending on the compliance status of the patches or extensions that you want to stage.

Patches cannot be staged if they are obsoleted by other patches in the baselines or baseline groups for the same stage operation. vSphere Lifecycle Manager stages only the patches that it can install in a subsequent remediation process, based on the current compliance status of the host. If a patch is obsoleted by patches in the same selected patch set, the obsoleted patch is not staged.

If a patch is in conflict with the patches in the vSphere Lifecycle Manager depot and is not in conflict with a host, after a compliance check, vSphere Lifecycle Manager reports this patch as a conflicting one. You can still stage the patch to the host and after the stage operation, vSphere Lifecycle Manager reports this patch as staged.

During the stage operation, vSphere Lifecycle Manager performs pre-scan and post-scan operations and updates the compliance status of the baseline.

For more information about the different compliance statuses that an update might have, see Compliance Statuses of Updates.

After you stage patches or extensions to hosts, you must remediate the hosts against all staged patches or extensions.

After remediation finishes, the host deletes all staged patches or extensions from its cache regardless of whether they were applied during the remediation. The compliance status of the patches or extensions that were staged but not applied to the hosts reverts from Staged to its previous value.

Important Staging patches and extensions is supported for hosts that are running ESXi 6.7 and later. You can stage patches to PXE booted ESXi hosts, but if the host is restarted before remediation, the staged patches are lost and you must stage them again.

Prerequisites

- Attach a patch or extension baseline or a baseline group containing patches and extensions to the host.
- Required privileges: **VMware vSphere Lifecycle Manager.Manage Patches and Upgrades.Stage Patches and Extensions**.

Procedure

1 In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.

   a Navigate to a host, cluster, or a container object.

   b Click the **Updates** tab.

2 Select **Hosts > Baselines**.

3 In the **Attached Baselines** pane, select one or more baselines.

4 Click **Stage**.

   The **Stage Patches** dialog box opens.

5 Select hosts on which to stage patches and extensions.

   The number of selected hosts is on the top of the list.

6 To view the patches or extensions that will download to the selected hosts, expand the **Stage** list.

7 Click **Stage**.

Results

The staging operation starts. You can monitor the progress of the task in the **Recent Tasks** pane.

What to do next

Remediate the host or hosts.

After remediation, all staged patches and extensions, whether installed or not during the remediation, are deleted from the host.

Remediating ESXi Hosts Against vSphere Lifecycle Manager Baselines and Baseline Groups

Remediation is the process during which vSphere Lifecycle Manager applies patches, extensions, and upgrades to ESXi hosts. Remediation makes the selected vSphere objects compliant with the attached baselines and baseline groups.

General Considerations

- vSphere Lifecycle Manager supports the remediation of ESXi hosts against patch, extension, and upgrade baselines.
- You can initiate remediation manually or schedule a regular remediation task to run at a time that is convenient for you.
- You can remediate a single ESXi host or multiple hosts in a container object. You can initiate remediation at a folder, a cluster, a data center, and even vCenter Server level.

  Note If you initiate remediation against a baseline for an object that contains clusters that use a single vSphere Lifecycle Manager image, remediation is not performed on those clusters.

- By default, the remediation process runs sequentially. That is, vSphere Lifecycle Manager remediates the hosts in a cluster or another container object one by one. However, you can configure vSphere Lifecycle Manager to remediate multiple hosts in parallel.
- If a vCenter Server instance is connected to other vCenter Server systems by a common vCenter Single Sign-On domain, you can remediate only the inventory objects managed by the vCenter Server system where the vSphere Lifecycle Manager instance that you use runs.
- To remediate vSphere objects against baselines or baseline groups, you must have the **Remediate to Apply Patches, Extensions, and Upgrades** privilege. For more information about managing users, groups, roles, and permissions, see the *vSphere Security* documentation.

  For a list of all vSphere Lifecycle Manager privileges and their descriptions, see vSphere Lifecycle Manager Privileges For Using Baselines.

- If a vCenter HA failover is initiated during the remediation of a cluster, the remediation task is canceled. After the failover finishes, you must restart the remediation task on the new node.

Orchestrated Upgrades of ESXi Hosts

You can use baseline groups to perform an orchestrated upgrade of the ESXi hosts in your environment. The baseline group might contain a single host upgrade baseline and multiple patch or extension baselines, or multiple patch and extension baselines. vSphere Lifecycle Manager first upgrades the hosts and then applies the patch or extension baselines. Because the upgrade runs first and patches are applicable to a specific host version, the orchestrated workflow ensures that no patches are lost during the upgrade.

Orchestrated upgrades can be performed at a host, cluster, folder, or a data center level.

Instead of creating a baseline group, you can select and work with multiple baselines instead of grouping them into a baseline group first.

Maintenance Mode

If the update requires it, vSphere Lifecycle Manager puts hosts into maintenance mode during remediation. Virtual machines cannot run when a host is in maintenance mode. To ensure a consistent user experience, vCenter Server migrates the virtual machines to other hosts within the cluster before the host is put in maintenance mode. vCenter Server can migrate the virtual machines if the cluster is configured for vMotion and if VMware Distributed Resource Scheduler (DRS) and VMware Enhanced vMotion Compatibility (EVC) are enabled. However, EVC is not a prerequisite for vMotion. EVC guarantees that the CPUs of the hosts are compatible. For container objects or individual hosts that are not in a cluster, migration with vMotion cannot be performed. After remediation, hosts exit maintenance mode. In case of failure during remediation, hosts might be unable to exit maintenance mode.

Parallel Remediation

You can enable vSphere Lifecycle Manager to remediate in parallel the hosts within a cluster that uses baselines. Parallel remediation reduces the time needed for patching or upgrading the hosts in your environment. You can remediate in parallel only ESXi hosts that are already in maintenance mode. During parallel remediation, hosts do not enter maintenance mode automatically. Similarly, after remediation finishes, the hosts do not exit maintenance mode automatically. To remediate hosts in parallel, you must manually enter and exit maintenance mode. If you enable parallel remedation, vSphere Lifecycle Manager does not remediate the ESXi hosts that are not in maintenance mode.

When you configure vSphere Lifecycle Manager to remediate hosts in parallel, you can set the maximum number of hosts to be remediated in a single remediation task. Alternatively, you can let vSphere Lifecycle Manager to remediate all hosts in maintenance mode in parallel.

When you remediate hosts in parallel, if the remediation of a single host fails, the remediation task for the entire cluster does not stop and the rest of the hosts are remediated successfully. After remediation finishes, vSphere Lifecycle Manager reports an error for the respective host.

Parallel remediation is deactivated by default, but you can enable it during remediation or in the vSphere Lifecycle Manager general remediation settings.

You cannot remediate in parallel hosts in a vSAN cluster.

Remediation Pre-Check

Before you remediate an object, you can perform a remediation pre-check on the object. During that check, vSphere Lifecycle Manager identifies possible issues that might prevent successful remediation and takes or suggests actions to fix the issues.

For more information about the possible issues that might prevent successful remediation, see Remediation Pre-Check Report.

Remediation of PXE Booted ESXi Hosts

vSphere Lifecycle Manager lets you remediate PXE booted ESXi hosts. vSphere Lifecycle Manager does not apply the patches that require a reboot to PXE booted ESXi hosts.

If there is any additional software installed on the PXE booted ESXi host, the software might be lost if the host restarts. Update your image profile with the additional software so that it will be present after the reboot.

To patch PXE booted ESXi hosts, you must enable the respective setting in the **Edit Settings for Host Remediation** dialog box, which you open from the **Settings** tab in the vSphere Lifecycle Manager home view.

Understanding the Remediation Operation

For ESXi hosts, updates are all-inclusive. The most recent update contains the patches from all previous releases.

The ESXi image on the host maintains two copies. The first copy is in the active boot and the second one is in the standby boot. When you patch an ESXi host, vSphere Lifecycle Manager creates an image based on the content of the active boot and the content of the patch. The new ESXi image is then located in the standby boot and vSphere Lifecycle Manager designates the active boot as the standby boot and reboots the host. When the ESXi host reboots, the active boot contains the patched image and the standby boot contains the previous version of the ESXi host image.

When you upgrade an ESXi host, vSphere Lifecycle Manager replaces the backup image of the host with the new image and replaces the active boot and the standby boot. During the upgrade, the layout of the disk that hosts the boots changes. The total disk space for an ESXi host remains 1GB, but the disk partition layout within that 1GB disk space changes to accommodate the new size of the boots where the ESXi 8.0 image is stored.

For rollback purposes, the term update refers to all ESXi patches, updates, and upgrades. Each time you update an ESXi host, a copy of the previous ESXi build is saved on your host.

If an update fails and the ESXi 8.0 host cannot boot from the new build, the host reverts to booting from the original boot build. ESXi permits only one level of rollback. Only one previous build can be saved at a time. In effect, each ESXi 8.0 host stores up to two builds, one boot build and one standby build.

The remediation of ESXi 6.7 and 7.0 hosts to their respective ESXi update releases is a patching process, while the remediation of ESXi hosts from version 6.7 or 7.0 to 8.0 is an upgrade process.

From the vSphere Lifecycle Manager settings, you can configure the host remediation process to skip a host reboot during host patch and host upgrade operations. This configuration setting is called Quick Boot. For more information about configuring the vSphere Lifecycle Manager remediation settings, see Chapter 3 vSphere Lifecycle Manager Remediation Settings.

Types of Host Remediation

Host remediation runs in different ways depending on the types of baselines that you attach to an object and whether the remediated host is in a cluster or not.

Host Upgrade Remediation

When you upgrade an ESXi6.7 or ESXi7.0 host to ESXi8.0, all supported custom VIBs remain intact on the host after the upgrade, regardless of whether the VIBs are included in the installer ISO.

You can upgrade hosts by using custom ESXi images that contain third-party modules for ESXi8.0. In such a case, third-party modules that are compatible with ESXi8.0 stay available on the upgraded host.

Host upgrade in a high-latency network in which vSphere Lifecycle Manager and the hosts are at different locations might take a few hours because the upgrade file is copied from the vSphere Lifecycle Manager depot to the host before the upgrade. During this time, the host stays in maintenance mode.

vSphere Lifecycle Manager 8.0 supports upgrade from ESXi 6.7 and ESXi 7.0 to ESXi 8.0.

Upgrading to ESXi8.0 requires a boot device that is a minimum of 4 GB. When booting from a local disk, SAN or iSCSI LUN, up to 128 GB of disk space is used to create ESXi system partitions. You can create a VMFS datastore on a boot disk larger than 128 GB.

Note After you upgrade your host to ESXi8.0, you cannot roll back to the previous ESXi versions, ESXi6.7, ESXi7.0. So, back up your host configuration before performing an upgrade. If the upgrade fails, you can reinstall the ESXi6.7 or ESXi7.0 software that you upgraded from and restore your host configuration. For more information about backing up and restoring your ESXi configuration, see the *VMware ESXi Upgrade* documentation. To upgrade ESXi hosts, you must first import ESXi ISO images to the vSphere Lifecycle Manager depot. You then create baselines and baseline groups to manage the upgrades for the ESXi hosts.

Host Patch Remediation

Patching is the process of remediating ESXi hosts against patch baselines.

The remediation of ESXi 6.7 and 7.0 hosts to their respective ESXi update releases is a patching process, while the remediation of ESXi hosts from version 6.7 or 7.0 to 8.0 is an upgrade process.

vSphere Lifecycle Manager handles host patches in the following ways:

- If a patch in a patch baseline requires the installation of another patch, vSphere Lifecycle Manager detects the prerequisite in thedepot and installs it together with the selected patch.
- If a patch is in a conflict with other patches that are installed on the host, the conflicting patch might not be staged or installed. However, if another patch in the baseline resolves

the conflicts, the conflicting patch is installed. For example, consider a baseline that contains patch A and patch C, and patch A conflicts with patch B, which is already installed on the host. If patch C obsoletes patch B, and patch C is not in a conflict with patch A, the remediation process installs patches A and C.

- If a patch is in a conflict with the patches in the vSphere Lifecycle Manager depot and is not in a conflict with the host, after a compliance check, vSphere Lifecycle Manager reports this patch as a conflicting one. You can stage and apply the patch to the host.
- When multiple versions of the same patch are selected, vSphere Lifecycle Manager installs the latest version and skips installing the earlier versions.

During patch remediation, vSphere Lifecycle Manager automatically installs the prerequisites of the patches.

With vSphere Lifecycle Manager8.0, you can remediate hosts of version ESXi6.7 and ESXi7.0 against patches from offline bundles, which you import to the vSphere Lifecycle Manager depot manually.

You can stage patches before remediation to reduce host downtime.

Host Extension Remediation

During extension remediation, vSphere Lifecycle Manager does not automatically install the prerequisites of the extension. Missing extension prerequisites cause some remediation operations to fail. If the missing prerequisite is a patch, you can add it to a patch baseline. If the missing prerequisite is an extension, you can add it to the same or another extension baseline. You can then remediate the host against the baseline or baselines that contain the prerequisite and the original extension baseline.

Remediating Hosts in a Cluster

For ESXi hosts in a cluster, the remediation process is sequential by default.

When you remediate a cluster of hosts sequentially and one of the hosts fails to enter maintenance mode, vSphere Lifecycle Manager reports an error and the remediation process stops and fails. The hosts in the cluster that are remediated stay at the updated level. The ones that are not remediated after one host fails remain unupdated.

The host upgrade remediation of ESXi hosts in a cluster proceeds only if all hosts in the cluster can be upgraded.

If you initiate remediation at a data center level, the remediation processes for the clusters run in parallel. Clusters that you manage with a single vSphere Lifecycle Manager image are not remediated against the attached baselines or baseline groups. If the remediation process fails for one of the clusters within a data center, the remaining clusters are still remediated.

Before you start remediation, you can generate a report that shows which cluster, host, or virtual machine has the cluster features enabled. For more information, see Remediation Pre-Check Report.

Remediation and Cluster Settings

If a host in a DRS-enabled cluster runs a virtual machine on which vCenter Server is installed, DRS first attempts to migrate the virtual machine running vCenter Server to another host, so that the remediation succeeds. If the virtual machine cannot be migrated to another host, the remediation fails for the host, but the remediation process for the cluster does not stop. vSphere Lifecycle Manager proceeds to remediate the next host in the cluster.

Remediation of hosts in a cluster requires that you temporarily deactivate cluster features such as VMware DPM and HA admission control. Also, you must turn off Fault Tolerance if it is enabled on any of the virtual machines on a host, and disconnect the removable devices connected to the virtual machines on a host, so that they can be migrated with vMotion. For more information about configuring the vSphere Lifecycle Manager remediation settings, see Chapter 3 vSphere Lifecycle Manager Remediation Settings.

If a vCenter HA failover is initiated during the remediation of a cluster, the remediation task is canceled. After the failover finishes, you must restart the remediation task on the new node.

When you perform remediation on a cluster that consists of not more than two hosts, deactivating HA admission control might not be enough to ensure successful remediation. You might need to deactivate vSphere High Availability (HA) for the cluster. If you keep HA enabled, the remediation attempts on hosts in the cluster fail, because HA cannot provide recommendation to vSphere Lifecycle Manager to place any of the hosts into maintenance mode. The reason is that if one of the two hosts is placed into maintenance mode there is no failover host left available in the cluster. To ensure successful remediation on a two-node cluster, you must deactivate HA for the cluster or place the hosts in maintenance mode manually and then remediate the two hosts in the cluster.

vSAN Clusters

vSphere Lifecycle Manager remediates hosts that are part of a vSAN cluster sequentially. The reason is that by design only one host from a vSAN cluster can be in a maintenance mode at any time. For more information about using vSphere Lifecycle Manager with vSAN clusters, see vSAN Clusters and vSphere Lifecycle Manager.

Remediating Hosts That Contain Third-Party Software

Hosts might contain third-party software, such as Cisco Nexus 1000V VEMs or EMC PowerPath modules. When you upgrade an ESXi6.7 or ESXi7.0 host to ESXi8.0, all supported custom VIBs are migrated and remain intact, regardless of whether the VIBs are included in the installer ISO.

If the host or the installer ISO image contains a VIB that creates a conflict and prevents the upgrade, an error message identifies the VIB that creates the conflict.

To discover potential problems with third-party software before an upgrade operation, scan the hosts against an upgrade baseline and review the scan messages in the vSphere Lifecycle Manager compliance view. See Host Upgrade Compliance Messages and Host Upgrade Compliance Messages When Cisco Nexus 1000V Is Present.

For information about upgrading with third-party customization, see the *VMware ESXi Upgrade* documentation.

For information about using vSphere ESXi Image Builder to make a custom ISO, see the *VMware ESXi Installation and Setup* documentation.

Remediating ESXi 6.7 or ESXi 7.0 Hosts Against an ESXi 8.0 Image

When you upgrade an ESXi 6.7 or ESXi 7.0 host to ESXi 8.0, all supported custom VIBs remain intact on the host after the upgrade, regardless of whether the VIBs are included in the installer ISO.

When you perform a compliance check, the target host is scanned against a set of VIBs from the upgrade image. If you check the compliance of a host against an upgrade baseline that contains an ISO image of the same version as the target host, vSphere Lifecycle Manager displays Compliant or Non-compliant compliance status. If the upgrade image is the basic one distributed by VMware, or is a custom ISO image that contains the same set of VIBs as the ones already installed on the target host, the scan result is Compliant. If the upgrade ISO contains VIBs that are of different kind or version than the VIBs that are already on the target host, the scan result is Non-compliant.

The remediation process of an ESXi 6.7 or ESXi 7.0 host against an ESXi 8.0 image is an upgrade process.

Note Upgrading to ESXi 8.0 requires a boot device that is a minimum of 4 GB. When booting from a local disk, SAN or iSCSI LUN, up to 128 GB of disk space is used to create ESXi system partitions. You can create a VMFS datastore on a boot disk larger than 128 GB.

You can use an ISO 8.0 image in an upgrade operation of an ESXi 8.0 host. The remediation process of ESXi 8.0 host by using ESXi 8.0 image with additional VIBs is equivalent to a patching process. Because the upgrade image is of the same version as the target host, upon completing the upgrade operation, the additional VIBs are added to the target host.

Table 8-4. Scan and Remediation Situations for ESXi 6.7 and ESXi 7.0 Hosts Against ESXi 8.0 Images

Action	Description
Compliance check and remediation of ESXi 6.7 or ESXi 7.0 hosts against an ESXi 8.0 image that contains additional non-conflicting and non-obsoleting VIBs with the target host.	vSphere Lifecycle Manager displays a Non-Compliant compliance status for the host. Remediation succeeds. All VIBs on the target host before remediation remain on the host. All VIBs from the upgrade image that are not present on the target host before remediation are added to the host.
Compliance check and remediation of ESXi 6.7 or ESXi 7.0 hosts against an ESXi 8.0 image that contains VIBs of a version later than the version of the same VIBs on the target host.	vSphere Lifecycle Manager displays a Non-Compliant compliance status for the host. Remediation succeeds. VIBs on the target host are updated to the later version.

Table 8-4. Scan and Remediation Situations for ESXi 6.7 and ESXi 7.0 Hosts Against ESXi 8.0 Images (continued)

Action	Description
Compliance check and remediation of ESXi 6.7 or ESXi 7.0 hosts against an ESXi 8.0 image that contains conflicting VIBs with the target host.	vSphere Lifecycle Manager displays an Incompatible compliance status for the host. Remediation fails. The host remains intact.
Scan and remediation of ESXi 6.7 or ESXi 7.0 hosts against an ESXi 8.0 image that contains vendor-tagged VIBs.	■ If the vendor-tagged VIBs do not match the host hardware, vSphere Lifecycle Manager displays an Incompatible compliance status for the host. Remediation fails. ■ If the vendor-tagged VIBs match the host hardware, vSphere Lifecycle Manager displays a Non-Compliant compliance status for the host and remediation succeeds.
Scan and remediation of ESXi 6.7 or ESXi 7.0 hosts against an ESXi 8.0 image that contains VIBs that obsolete the VIBs installed on the host.	Remediation succeeds. All VIBs that have been installed on the target host before remediation are replaced by the newer VIBs from the ESXi image.

Generate a Pre-Remediation Check Report

When you generate a pre-remediation check report, vSphere Lifecycle Manager generates a list with actions that you must perform to ensure successful remediation of the hosts in your cluster.

The remediation pre-check report contains information about issues at the cluster, host, and VM level that might prevent the completion of remediation.

For information about the possible issues that might prevent successful remediation, see Remediation Pre-Check Report.

Procedure

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
    a. Navigate to a host, cluster, or a container object.
    b. Click the **Updates** tab.
2. Select **Host > Baselines**.
3. In the **Baselines** pane, click **Pre-Check Remediation**.

    The **Remediation Pre-check** dialog box opens.
4. Review the results from the pre-check and click **Done**.

    In the bottom pane of the **Remediation Pre-check** dialog box, you see a list of issues at the host and virtual machine level.

Results

The **Remediation Pre-check** dialog box lists the issues with cluster, hosts, and virtual machines that might prevent successful remediation of the selected object.

In the upper pane of the **Remediation Pre-check** dialog box, you see a list of issues at a cluster level.

In the bottom pane of the **Remediation Pre-check** dialog box, you see a list of issues at the host and virtual machine level.

What to do next

Fix all issues that vSphere Lifecycle Manager identifies during the pre-remediation check and remediate the selected object.

Remediation Pre-Check Report

The remediation pre-check report shows the results of a check that is performed on a cluster or a host before remediation. During that check, vSphere Lifecycle Manager identifies possible issues that might prevent successful remediation. Depending on the type of issue, vSphere Lifecycle Manager suggests actions that you must take to fix the issue or resolves the issue automatically.

You can generate a pre-check remediation report in the vSphere Lifecycle Manager compliance view for an object.

Table 8-5. Cluster Issues

Current Configuration/ Issue	Recommended Action	Details
DRS is deactivated on the cluster.	Enable DRS on the cluster.	DRS enables vCenter Server to place and migrate virtual machines automatically on hosts to attain the best use of cluster resources.
vSAN health check fails during the pre-check.	Navigate to the vSAN Health page and address any health issues before proceeding with remediation.	The vSAN health check performs a series of tests on the hosts in the vSAN cluster. The vSAN health check must succeed to ensure the hosts are successfully remediated. If you start a remediation task in a vSAN cluster that failed the vSAN health check during the remediation pre-check, the hosts enter maintenance mode, get upgraded, but might fail to exit maintenance mode. The remediation eventually fails.
Insufficient licenses for one or multiple ESXi hosts in the cluster.	Ensure that you have multiple licenses for the ESXi hosts that have more than 32 cores per CPU.	One CPU license covers up to 32 physical cores. If a CPU has more than 32 cores, you must assign additional CPU licenses to the respective ESXi host. For more information, see https://www.vmware.com/company/news/updates/cpu-pricing-model-update-feb-2020.html.
DPM is enabled on the cluster.	None. vSphere Lifecycle Manager deactivates DPM automatically.	If a host has no running virtual machines, DPM might put the host in standby mode before or during remediation and vSphere Lifecycle Manager cannot remediate them.
HA admission control is enabled on the cluster.	None. vSphere Lifecycle Manager deactivates HA admission control automatically.	HA admission control prevents the migration of virtual machines with vSphere vMotion and the hosts cannot enter maintenance mode.

Table 8-6. Host Issues

Current Configuration/Issue	Recommended Action	Details
A CD/DVD drive is attached to a virtual machine on the ESXi host.	Disconnect the CD/DVD drive.	Any CD/DVD drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
A floppy drive is attached to a virtual machine on the ESXi host.	Disconnect the floppy drive.	Any floppy drives or removable devices connected to the virtual machines on a host might prevent the host from entering maintenance mode. When you start a remediation operation, the hosts with virtual machines to which removable devices are connected are not remediated.
Fault Tolerance (FT) is enabled for a virtual machine on the ESXi host.	Deactivate FT for the virtual machine.	If FT is enabled for any of the virtual machines on a host, vSphere Lifecycle Manager cannot remediate that host.
A powered on virtual machine is configured to use Virtual Flash Read Cache.	Deactivate Virtual Flash Read Cache before proceeding with the upgrade.	Virtual Flash Read Cache is not supported. During an upgrade operation, vSphere Lifecycle Manager removes Virtual Flash Read Cache for all virtual machines on the host. Before remediation, consult https://kb.vmware.com/s/article/2057840.
VMware vCenter Server is installed on a virtual machine on the ESXi host and DRS is deactivated on the cluster.	Enable DRS on the cluster and ensure that virtual machines can be migrated with vSphere vMotion.	One of the virtual machines in the cluster runs the vCenter Server instance that you currently use. If you enable DRS on the cluster, vSphere vMotion can migrate the virtual machine where vCenter Server runs to ensure that the remediation of the hosts is successful.
An ESXi host in the cluster has a CPU with more than 32 cores and requires multiple licenses.	Assign as many licenses as the host needs.	One CPU license covers up to 32 physical cores. If a CPU has more than 32 cores, you must obtain additional CPU licenses. For more information, see https://www.vmware.com/company/news/updates/cpu-pricing-model-update-feb-2020.html.

Remediate ESXi Hosts Against a Single Baseline or Multiple Baselines

Remediation makes the remediated ESXi host compliant with the attached baselines and baseline groups. You can remediate a host against a single or multiple baselines, or against a baseline group. Baseline groups might contain multiple patch and extension baselines, or an upgrade baseline combined with multiple patch and extension baselines. You can remediate ESXi hosts against a single attached upgrade baseline at a time.

You can upgrade all hosts in your vSphere inventory by using a single upgrade baseline that contains an ESXi image. You can remediate a single ESXi host or a group of ESXi hosts in a container object, such as a folder, a cluster, or a data center. You can also initiate remediation at a vCenter Server level.

Note Because the official VMware online depot hosts certified partner content in addition to VMware content, a broader set of OEM bulletins are available in the vSphere Lifecycle Manager depot. As a result, a broader set of OEM bulletins are included in the vSphere Lifecycle Manager predefined bulletins. During remediation, always inspect the contents of those baselines to exclude the bulletins that you do not need in the baseline. For the bulletins that you do need, consult the corresponding KB articles for information about deployment specifics and dependencies. Verify that dependent bulletins are also included in the baselines that you use for remediation.

Prerequisites

- Required privileges: **VMware vSphere Lifecycle Manager.Manage Patches and Upgrades.Remediate to Apply Patches, Extensions, and Upgrades**.
- Attach a patch, upgrade, or extension baseline or a baseline group containing patches, upgrades, and extensions to the host.
- Resolve any issues that occur during Remediation Pre-check.
- In upgrade scenarios, verify that the ESXi hosts to upgrade have a boot disk of at least 4 GB. When booting from a local disk, SAN or iSCSI LUN, up to 128 GB of disk space is used to create ESXi system partitions. You can create a VMFS datastore on a boot disk larger than 128 GB.
- To enable Quick Boot, verify that the ESXi host is compatible with the feature. For more information, see Quick Boot.

Procedure

1. In the vSphere Client, navigate to the vSphere Lifecycle Manager compliance view for an individual host or a container object.
   a. Navigate to a host, cluster, or a container object.
   b. Click the **Updates** tab.
2. Select **Hosts > Baselines**.
3. In the **Attached Baselines and Baseline Groups** pane, select the baselines and baseline groups to use for remediation.

   You can select a single baseline or baseline group. You can also select multiple baselines and baseline groups. Your selection must contain no more than one upgrade baseline.

4 Click **Remediate**.

If the selected baselines and baseline groups do not contain an upgrade image, the **Remediate** dialog box opens.

If the selected baselines and baseline groups contain an upgrade image, the **End User License Agreement** dialog box opens.

5 To proceed to remediation, accept the terms and the license agreement in the **End User License Agreement** dialog box.

After you accept the agreement and click **OK** to close the dialog box, the **Remediate** dialog box opens.

6 Expand the list of pre-check issues and review the actions that vSphere Lifecycle Manager must perform to ensure successful remediation.

7 (Optional) To generate a full remediation pre-check report, click **Show Full Remediation Pre-Check Report**.

If you select this option, the **Remediate** dialog box closes and vSphere Lifecycle Manager does not proceed with the remediation process. Instead, the **Remediation Pre-Check** dialog box opens. After you review the results from the remediation pre-check, you must initiate remediation again.

8 Expand the list of hosts to be remediated and deselect any host that you do not want to remediate.

The list contains all the hosts to which the selected baselines and baseline groups are attached. Even if you navigated to a single host before initiating remediation, the list might still display multiple hosts to be remediated. All hosts in the list are selected by default. Deselecting hosts from the list changes the overall number of hosts to be remediated.

9 (Optional) To view information about the updates that will be installed during the remediation, expand the list of updates.

If the selection of baselines and baseline groups contains an upgrade baseline, information about the ESXi image is also displayed.

10 (Optional) To schedule the remediation task for a later time, expand **Scheduling Options** and configure a scheduled remediation task.

By default, the remediation task starts immediately after closing the **Remediate** dialog box.

11 Expand **Remediation settings** and review and edit the remediation settings.

- To turn on or turn off Quick Boot, select or deselect the respective check box in the **Remediation settings** table.
- To allow or disallow health checks after remediation, select or deselect the respective check box in the **Remediation settings** table.
- To ignore warnings about unsupported hardware devices, select the respective check box in the **Remediation settings** table.

- To configure parallel remediation for the selected hosts, expand **Parallel remediation**, select the respective check box and configure the maximum number of concurrent remediations.

  Note vSphere Lifecycle Manager remediates in parallel only the ESXi hosts that are in maintenance mode. Hosts that are not in maintenance mode are not remediated. If you do not set the maximum number of concurrent remediations, vSphere Lifecycle Manager remediates all hosts that are in maintenance mode.

  If the hosts have NSX virtual distributed switches that are ready to be migrated to vSphere Distributed Switches, you must set the maximum number of parallel remediations to no more than 4. In cases when host switch migration is needed, if more than 4 hosts are remediated in parallel, the remediation might fail, because the host switch migration takes more time than the time vSphere Lifecycle Manager needs to complete the parallel remediation.

- To change any other of the remediation settings, click the **Close Dialog And Go To Settings** link above the table.

  If you select this option, the **Remediate** dialog box closes and vSphere Lifecycle Manager does not proceed with the remediation process. Instead, you are redirected to the **Baselines Remediation Settings** pane on the **Settings** tab of the vSphere Lifecycle Manager home view. To change any of the remediation settings, click the **Edit** button. Remediation does not resume automatically. After you make the desired changes, you must initiate remediation again.

12 Click **Remediate**.

Results

Depending on the remediation schedule you configure, the remediation task starts immediately or runs later.

Using vSphere Lifecycle Manager to Migrate an NSX Virtual Distributed Switch to a vSphere Distributed Switch

Starting with vSphere 7.0, the vSphere Distributed Switch supports the NSX functionality. For clusters enabled with NSX, you can migrate the NSX-managed Virtual Distributed Switches on the hosts to vSphere Distributed Switches during an upgrade of a cluster against a vSphere Lifecycle Manager baseline group that contains an ESXi image and NSX VIBs .

Migrating your host switch to vSphere Distributed Switch 7.0 or later ensures optimal pNIC usage, and lets you manage the networking for your NSX hosts from vCenter Server.

During an upgrade remediation, vSphere Lifecycle Manager checks if an NSX virtual distributed switch is present on each of the hosts in the cluster and if it is ready to be migrated. To prepare the NSX virtual distributed switch for migration, you must run the Upgrade Readiness Tool before upgrading the cluster. If the NSX distributed switch on any of hosts in the cluster is not ready to be migrated to a vSphere Distributed Switch, you cannot proceed with the remediation process. In this case, you need to go to NSX Manager and run the Upgrade Readiness Tool.

Requirements

- ESXi 7.0 Update 2
- vCenter Server 7.0 Update 2
- NSX 3.1.1

As a good practice, contact VMware support to assess the impact of migrating to vSphere Distributed Switch 7.0 or later.

Workflow

1 In NSX Manager, use the Upgrade Readiness Tool to run the migration readiness pre-check, address any configuration issues, review the recommended topology, and apply the new topology.

   For more information about the steps you need to perform in NSX Manager, see "Migrate Host Switch to vSphere Distributed Switch" in the *NSX Center Administration* documentation.

2 Upgrade vCenter Server to version 7.0 Update 2.

   For more information about upgrading vCenter Server, see the *vSphere Upgrade* documentation.

3 Create a baseline group that contains an ESXi image version 7.0 Update 2 and the NSX kernel module for ESXi 7.0 .

   a Import an ESXi 7.0 Update 2 ISO image to the vSphere Lifecycle Manager depot.

      For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.

   b Create an upgrade baseline that contains the imported ISO image.

      For more information, see Create, Edit, or Delete vSphere Lifecycle Manager Baselines and Baseline Groups .

   c From customerconnect.vmware.com, download the NSX kernel module for ESXi 7.0.

   d Import the downloaded NSX bundle to the vSphere Lifecycle Manager depot.

      For more information, see Import Updates to the vSphere Lifecycle Manager Depot.

   e Create an extension baseline that contains the imported kernel module.

      For more information, see Create, Edit, or Delete vSphere Lifecycle Manager Baselines and Baseline Groups .

   f Create a baseline group that contains the ESXi upgrade baseline and the extension baseline with NSX VIBs.

   For more information, see Create a Host Baseline Group.

4 Attach the baseline group to a cluster.

   For more information, see Attach Baselines and Baseline Groups to Objects.

5 Remediate the cluster against the attached baseline group.

   During the remediation, vSphere Lifecycle Manager upgrades the ESXi version first and then migrates the host switch, if migration is needed.

   For more information, see Remediate ESXi Hosts Against a Single Baseline or Multiple Baselines.

6 If you use host profiles to configure the hosts in your environment, re-extract a new host profile from the reference host in the cluster.

   After the upgrade, due to the migration of the host switch, the existing host profiles become invalidated and inapplicable.

   For more information, see the *vSphere Host Profiles* documentation.

Upgrading Virtual Machines with vSphere Lifecycle Manager

9

You can use vSphere Lifecycle Manager to upgrade virtual machine hardware and the VMware Tools version of a virtual machine.

Whether you perform an upgrade of the virtual machine hardware version or the VMware Tools version, the upgrade is a multi-stage process.

1 You check the status of individual virtual machines or a container object.

   vSphere Lifecycle Manager checks the status of a virtual machine against the latest virtual machine hardware version supported by the host on which the virtual machine runs. Similarly, vSphere Lifecycle Manager checks the status of the virtual machine against the latest VMware Tools version supported by the host on which the virtual machine runs.

   For more information about checking virtual machine status, see Checking the Status of Virtual Machines.

2 You review the status of the scanned virtual machines.

3 You upgrade the virtual machine to match the host where it resides.

   With vSphere Lifecycle Manager, you can upgrade the virtual machine hardware version and the VMware Tools version that a virtual machine has. You can use vSphere Lifecycle Manager to upgrade the virtual machine hardware version to the latest hardware version, vmx-19, and to the latest VMware Tools version on the hosts.

   For more information about upgrading virtual machines, see Upgrading Virtual Machines.

Read the following topics next:

- Configure Virtual Machine Rollback Settings
- Checking the Status of Virtual Machines
- Upgrading Virtual Machines

Configure Virtual Machine Rollback Settings

By default, vSphere Lifecycle Manager takes snapshots of virtual machines before upgrading them. If the upgrade fails, you can use the snapshot to return a virtual machine to its state before the upgrade.

You can configure vSphere Lifecycle Manager to keep snapshots for an indefinite or fixed period of time. Use the following guidelines when managing snapshots.

- Keeping snapshots indefinitely might consume a large amount of disk space and degrade virtual machine performance.
- Keeping no snapshots saves space, ensures best virtual machine performance, and might reduce the remediation time. However, keeping no snapshots limits the availability of a rollback.
- Keeping snapshots for a fixed period of time uses less disk space and offers a backup for a short time.

vSphere Lifecycle Manager does not take snapshots of fault tolerant virtual machines and virtual machines of virtual machine hardware version 3. If you decide to take snapshots of such virtual machines, the upgrade might fail.

If you configure vSphere Lifecycle Manager to automatically upgrade VMware Tools on power cycle for selected virtual machines, vSphere Lifecycle Manager does not take snapshots of the virtual machines before upgrading them and you cannot roll back.

Prerequisites

Required privileges: **VMware vSphere Lifecycle Manager. Configure**

Procedure

1 Navigate to the vSphere Lifecycle Manager home view.

   a In the vSphere Client, select **Menu > Lifecycle Manager**.

   b Select a vCenter Server system from the **Lifecycle Manager** drop-down menu.

   The drop-down menu is available only when multiple vCenter Server systems are connected by a common vCenter Single Sign-On domain. By selecting a vCenter Server system, you specify which vSphere Lifecycle Manager instance you want to administer.

2 On the **Settings** tab, select **Cluster lifecycle > VMs**.

3 Click the **Edit** button.

   The **Edit Default Settings for VM Rollback** dialog box opens.

4 Select the **Take snapshot of VMs** check box.

5 Select the time period for keeping the snapshots.

   - Do not delete snapshots
   - Keep snapshots for a configurable, fixed period of time

6 Click **Save** to save your changes and close the **Edit Default Settings for VM Rollback** dialog box.

Results

These settings become the default rollback option settings for virtual machines. You can specify different settings when you configure individual remediation tasks.

Checking the Status of Virtual Machines

You use vSphere Lifecycle Manager to check the status of virtual machines before you upgrade them. The status check shows if the virtual machine is up-to-date or can be upgraded.

With vSphere Lifecycle Manager, you can check the status of a single virtual machine or a group of virtual machines in a parent container object.

Supported groups of virtual machines or ESXi hosts include virtual infrastructure container objects such as folders, vApps, clusters, and data centers.

vSphere Lifecycle Manager checks the status of virtual machines in two aspects.

- You can use vSphere Lifecycle Manager to check the status of the virtual machines in respect with the VMware Tools version that they have installed.

  The status check is performed against the latest VMware Tools version that the parent host supports.

- vSphere Lifecycle Manager checks the status of the virtual machines in respect with their VM hardware compatibility.

  vSphere Lifecycle Manager compares the hardware compatibility of the virtual machines with the default VM hardware compatibility configured for the host.

Check the Status of an Individual Virtual Machine

You check the status of virtual machines to see whether the VMware Tools version they have is up to date and whether their hardware compatibility matches the default VM hardware compatibility for the host.

Procedure

1. In the vSphere Client, navigate to a virtual machine.
2. On the **Updates** tab, click **Check Status**.

   The **Scan entity** task appears in the **Recent Tasks** pane. After the task finishes, status information appears in the **VMware Tools** and **VM Hardware Compatibility** panels.

Results

The virtual machines are scanned for VMware Tools and VM hardware compliance.

Check the Status of the Virtual Machines in a Container Object

You check the status of virtual machines to see whether the VMware Tools version they have is up-to-date and whether their hardware compatibility matches the default VM hardware compatibility for the host where they reside.

When you perform a status check for a container object, vSphere Lifecycle Manager checks the VMware Tools and VM Hardware Compatibility statuses for all child virtual machines. The larger the virtual infrastructure and the higher up in the object hierarchy you initiate the status check, the longer the task takes.

Procedure

1. In the vSphere Client, navigate to a virtual machine container object, such as a virtual machine folder, host, cluster, and so on.
2. Click the **Updates** tab.
3. Select your task.

Option	Action
Check the VMware Tools status of the virtual machines in the container object.	a Select **Hosts > VMware Tools >** . b Click **Check Status**. The information about the VMware Tools status appears in the **Tools Status** column in the table that lists all virtual machines in the selected container object. If the container object is a data center or a vCenter Server instance, you must first specify the cluster that you want to see results for.
Check the VM Hardware compatibility status of the virtual machines in the container object.	a Select **Hosts > VM Hardware**. b Click **Check Status**. The information about the VM Hardware Compatibility status appears in the **Status** column in the table that lists all virtual machines in the selected container object. For each virtual machine in the object, you can also see the VM hardware compatibility and the host compatibility. If the container object is a data center or a vCenter Server instance, you must first specify the cluster that you want to see results for.

The VMware Tools Status

Check the VMware Tools status for information whether the current version of VMware Tools is installed, supported, or whether upgrades are available.

Table 9-1. VMware Tools Status

VMware Tools Status	Description
Up to Date	VMware Tools is installed, supported, and the version is compliant.
	VMware Tools is installed, supported, and the version is newer than the version available on the ESXi host.

Table 9-1. VMware Tools Status (continued)

VMware Tools Status	Description
Upgrade Available	VMware Tools is installed, but the version is old.
	VMware Tools is installed and supported, but a newer version is available on the ESXi host.
Version Unsupported	VMware Tools is installed, but the version is old.
	VMware Tools is installed, but the version has a known issue and must be immediately upgraded.
	VMware Tools is installed, but the version is too new to work correctly with this virtual machine.
Not Installed	VMware Tools is not installed on this virtual machine.
Guest Managed	vSphere does not manage VMware Tools.
Unknown	The status of the virtual machine is not checked.

Upgrading Virtual Machines

With vSphere Lifecycle Manager, you can upgrade the VMware Tools version and the hardware version of a virtual machine. You can also upgrade multiple virtual machines simultaneously if the virtual machines are in a container object, such as a folder or vApp. You can also upgrade simultaneously all virtual machines that run on a host, in a cluster, or in a data center.

vSphere Lifecycle Manager supports upgrading powered on, suspended, and powered off virtual machines.

During the upgrade of VMware Tools, the virtual machines must be powered on. If a virtual machine is in the powered off or suspended state before remediation, vSphere Lifecycle Manager powers it on. After the upgrade completes, vSphere Lifecycle Manager restarts the machine and restores the original power state of the virtual machine.

During the virtual hardware upgrade, the virtual machines must be powered off. If a virtual machine is powered on, vSphere Lifecycle Manager powers the machine off, upgrades the virtual hardware, and then powers the virtual machine on.

You can also upgrade VMware Tools and the hardware version of a virtual machine template. A template is a copy of a virtual machine that you can use to create and provision new virtual machines.

You can set up automatic upgrades of VMware Tools on power cycle. For more information, see Automatically Upgrade VMware Tools on Reboot.

You can configure vSphere Lifecycle Manager to take snapshots of virtual machines and to keep the snapshots indefinitely or for a specific period of time. By using snapshots, you can roll back a virtual machine to its previous state if upgrading the virtual machine with vSphere Lifecycle Manager fails. After the upgrade finishes, you can delete the snapshots if you do not need them. For more information about configuring virtual machine rollback settings, see Configure Virtual Machine Rollback Settings.

You can upgrade virtual machines immediately or schedule an upgrade operation to run at a convenient time.

If a host is connected to vCenter Server by using an IPv6 address, you cannot scan and remediate virtual machines that run on the host.

Upgrade the VM Hardware Compatibility of Virtual Machines

You can upgrade the hardware of virtual machines to the latest hardware version that the host supports. You can upgrade immediately or schedule an upgrade at a time that is convenient for you.

With vSphere Lifecycle Manager, you can upgrade the hardware compatibility version of a single virtual machine or multiple virtual machines simultaneously. Supported container objects for virtual machines in the vSphere inventory are folders, vApps, data centers.

Procedure

1 In the vSphere Client, navigate to a single virtual machine or a container object.

   You can also initiate upgrade at the level of any inventory object where virtual machines run. For example, you can start the upgrade operation at a host or cluster level.

2 Open the **Upgrade VM Hardware to Match Host** dialog box.

Inventory Object	Steps
Virtual Machine	a Click the **Updates** tab. b In the **VM Hardware Compatibility** panel, click **Upgrade to Match Host**.
Container Object, Host, Cluster, Data Center, or vCenter Server Instance	a Click the **Updates** tab. b Select **Hosts > VM Hardware**. c If the selected inventory object is a data center or a vCenter Server instance, select a cluster from the list. A list of all virtual machines in the cluster appears in the bottom pane. d Select the virtual machines to upgrade. e Click **Upgrade to Match Host**.

   A list of the virtual machines selected for upgrading is visible in the **Upgrade VM Hardware to Match Host** dialog box.

3 (Optional) To change the selection of the virtual machines to upgrade, select or deselect virtual machines from the list.

4 (Optional) To schedule the upgrade for a specific date and time, expand **Scheduling Options** and configure the scheduled task.

   a Enter a name and, optionally, a description for the scheduled upgrade task.

   b Use the **Powered On VMs**, **Powered Off VMs**, and **Suspended VMs** drop-down menus to configure the upgrade to run immediately or at a specific date and time.

5 (Optional) To configure the use of snapshots, expand **Rollback Options** and change the default settings.

   a To allow or disallow taking of snapshots of virtual machines before upgrading them, select or deselect the **Take snapshot of VMs** check box.

      The option to take snapshots is selected by default.

   b Select a period for keeping the snapshots.

      - Keep the snapshots indefinitely.
      - Keep the snapshots for a fixed period.

   c Enter a snapshot name and, optionally, a description for the snapshot.

   d Include the virtual machine memory in the snapshot by selecting the respective check box.

6 Review your selections and click the **Upgrade to Match Host** button.

Results

The hardware versions of the selected virtual machines are upgraded and the virtual machine status changes to Up to Date.

Upgrade the VMware Tools Version of Virtual Machines

You can upgrade the VMware Tools version of virtual machines to the latest version that the host supports. You can upgrade immediately or schedule an upgrade at a time that is convenient for you.

With vSphere Lifecycle Manager, you can upgrade the VMware Tools version of a single virtual machine or multiple virtual machines simultaneously. Supported container objects for virtual machines in the vSphere inventory are folders, vApps, data centers.

Procedure

1 In the vSphere Client, navigate to a single virtual machine or a container object.

   You can initiate the upgrade at the level of any inventory object where virtual machines run. For example, you can start the upgrade operation at a host or cluster level.

2 Open the **Upgrade VMware Tools to Match Host** dialog box.

Inventory Object	Steps
Virtual Machine	a Click the **Updates** tab. b In the **VMware Tools** panel, click **Upgrade to Match Host**.
Container Object, Host, Cluster, Data Center, or vCenter Server Instance	a Click the **Updates** tab. b Select **Hosts > VMware Tools**. c If the selected inventory object is a data center or a vCenter Server instance, select a cluster from the list. A list of all virtual machines in the cluster appears in the bottom pane. d In the **VMs in Cluster** pane, select the virtual machines to upgrade. e Click **Upgrade to Match Host**.

A list of the virtual machines selected for upgrading is visible in the **Upgrade VMware Tools to Match Host** dialog box.

3 (Optional) To change the selection of the virtual machines to upgrade, select or deselect virtual machines from the list.

4 (Optional) To schedule the upgrade for a specific date and time, expand **Scheduling Options** and configure the scheduled task.

   a Enter a name and, optionally, a description for the scheduled upgrade task.

   b Use the **Powered On VMs**, **Powered Off VMs**, and **Suspended VMs** drop-down menus to configure the upgrade to run immediately or at a specific date and time.

5 (Optional) To configure the use of snapshots, expand **Rollback Options** and change the default settings.

   a To allow or disallow taking of snapshots of virtual machines before upgrading them, select or deselect the **Take snapshot of VMs** check box.

   The option to take snapshots is selected by default.

   b Select a period for keeping the snapshots.

   - Keep the snapshots indefinitely.
   - Keep the snapshots for a fixed period.

   c Enter a snapshot name and, optionally, a description for the snapshot.

   d Include the virtual machine memory in the snapshot by selecting the respective check box.

6 Review your selections and click the **Upgrade to Match Host** button.

Results

The VMware Tools version that runs on the selected virtual machines is upgraded and the VMware Tools status changes to Up to Date.

Automatically Upgrade VMware Tools on Reboot

You can automate the process of upgrading VMware Tools for the virtual machines in your inventory.

You can set up vSphere Lifecycle Manager to check the VMware Tools version of a virtual machine when the virtual machine is rebooted. If necessary, vSphere Lifecycle Manager upgrades VMware Tools to the latest version supported by the host on which the virtual machine runs.

Note When you perform a VMware Tools upgrade on power cycle, vSphere Lifecycle Manager does not take a snapshot of the virtual machine and you cannot roll back to the previous version of the virtual machine.

Prerequisites

Verify that you have the **Manage Patches and Upgrades.Remediate to Apply Patches, Extensions, and Upgrades** privilege.

Procedure

1 In the vSphere Client, navigate to a single virtual machine or an inventory object that contains virtual machines.

2 Configure vSphere Lifecycle Manager to automatically upgrade VMware Tools on reboot.

Inventory Object	Steps
Virtual machine	a Click the **Updates** tab. b In the **VMware Tools** panel, click **Turn On**.
Container Object, Host, cluster, data center, or vCenter Server instance	a Click the **Updates** tab. b Select **Hosts > VMware Tools**. c If the selected inventory object is a data center or a vCenter Server instance, select a cluster from the list. A list of all virtual machines in the cluster appears in the bottom pane. d In the **VMs in cluster** pane, select the virtual machines for which you want to enable the automatic upgrade of VMware Tools. e Click **Set Auto Update** and select **On**. The new status is visible in the **Auto Update** column.

Results

The next time you power on or restart a virtual machine, vSphere Lifecycle Manager checks the version of VMware Tools installed on the virtual machines and performs an upgrade, if necessary.

vSphere Lifecycle Manager Images and Other VMware Products and Solutions

10

You can use a vSphere Lifecycle Manager image to manage a cluster if the cluster only contains solutions integrated to work with vSphere Lifecycle Manager. If an unitegrated solution is enabled on a cluster, you cannot use vSphere Lifecycle Manager images to manage that cluster, but you can still use baselines and baseline groups.

A solution is a VMware product that integrates with vCenter Server and adds some new functionality to the ESXi hosts in the inventory.

When you enable a solution for a cluster that uses a vSphere Lifecycle Manager image, the solution automatically uploads an offline bundle with components into the vSphere Lifecycle Manager depot and adds its component to all hosts in the cluster. You cannot control the lifecycle of solution components. For example, if you export the image, solution components are not part of the exported image.

Integrated Solutions

You can manage a cluster with a single image if the cluster has any of the following solutions enabled.

- vSphere High Availability
- vSAN

  For more information about the integration between vSAN and vSphere Lifecycle Manager, see vSAN Clusters and vSphere Lifecycle Manager and the *Administering VMware vSAN* documentation.
- vSAN File Services
- vSphere IaaS control plane

  For detailed information about the integration between vSphere IaaS control plane and vSphere Lifecycle Manager, see the *vSphere with Tanzu Configuration and Management* documentation.
- NSX

  For more information about the integration between NSX and vSphere Lifecycle Manager, see the *NSX Administration* documentation.

- VMware Cloud Foundation

  vSphere Lifecycle Manager is available as an option in the VMware Cloud Foundation Workload Domain. For more information, see the *VMware Cloud Foundation Lifecycle Management* documentation.

- VMware vSphere Replication

  For more information about the integration between vSphere Lifecycle Manager and vSphere Replication, see the *vSphere Replication* documentation.

You can also use baselines for clusters that have those solutions enabled.

Unintegrated Solutions

You cannot manage a cluster with a single image if the cluster has any of the following solutions enabled.

- NSX for vSphere®
- Dell EMC VxRail

You can use baselines and baseline groups to manage clusters that have those solutions enabled.

Read the following topics next:

- vSAN Clusters and vSphere Lifecycle Manager
- vSphere Lifecycle Manager and vSphere IaaS control plane
- vSphere Lifecycle Manager and VMware NSX®

vSAN Clusters and vSphere Lifecycle Manager

You can manage a vSAN cluster by using vSphere Lifecycle Manager baselines and baseline groups or by using a single image for that cluster. Working with vSAN clusters has its specifics regardless of whether you manage the cluster with a single image or with baselines.

Managing a vSAN Cluster by Using Recommendation Baseline Groups

You can update and upgrade the hosts in a vSAN cluster by using automatically generated system-managed baselines groups. Those system-managed baseline groups are called recommendation baseline groups. Recommendation baseline groups do not contain firmware and driver updates. Recommendation baselines contain only patch or upgrade baselines.

If you want to switch to using images for a vSAN cluster that contains ESXi hosts of versions earlier than 7.0, you must first use an upgrade baseline to upgrade the hosts. Then, you can switch to using a vSphere Lifecycle Manager image for the cluster.

For more information about recommendation baselines, see About Recommendation Baseline Groups.

For more information about using baselines to manage hosts and clusters, see Chapter 8 Using vSphere Lifecycle Manager Baselines and Baseline Groups .

Managing a vSAN Cluster with a Single Image

The image that you use for a cluster defines the full software stack to run on the hosts in that cluster: ESXi version, vendor customization, drivers, and firmware. When you manage a vSAN cluster with a single image, you can take advantage of the functionalities that vSphere Lifecycle Manager images provide.

- You can update the firmware on all hosts in the vSAN cluster.

  You perform firmware update by setting up an image that contains a firmware add-on and remediating the vSAN cluster against that image. For more information about performing firmware updates by using vSphere Lifecycle Manager images, see Firmware Updates with vSphere Lifecycle Manager.

- You can run a hardware compatibility check for the cluster.

  The hardware compatibility check task verifies that the image for the cluster can be successfully applied to all hosts and that it is compliant with the vSAN Hardware Compatibility List (HCL). For more information about hardware compatibility checks, see Chapter 7 vSphere Lifecycle Manager Hardware Compatibility Checks for Clusters and Hosts.

- You can check firmware compliance with the image.

  When you perform a compliance check against the image for a cluster, firmware compliance is also checked. As a result, you can easily notice if a driver or firmware in your cluster becomes non-compliant. For more information about checking the compliance of a cluster against an image, see Check the Compliance Against a Single Image.

- You can use vSphere Lifecycle Manager recommended images.

  When you manage a vSAN cluster with vSphere Lifecycle Manager images, the vSAN recommendation engine does not generate vSAN health alarms or recommendation baselines for that cluster. However, vSphere Lifecycle Manager generates pre-validated images include a recommended firmware version for the hosts in your vSAN cluster. For more information about vSphere Lifecycle Manager recommended images, see vSphere Lifecycle Manager Recommended Images.

Managing a vSAN Witness Host with a Single Image

Starting with vSphere 8.0 Update 2, you can start managing a standalone vSAN witness host with a single image. The witness host can be dedicated to a vSAN stretched cluster or support up-to 64 two-node vSAN clusters. You upgrade a witness host that you manage with a vSphere Lifecycle Manager image in the same way you upgrade any other standalone host. For more information, see Chapter 6 How to Use vSphere Lifecycle Manager Images and vSphere Lifecycle Manager and the vSAN Witness Hosts.

Remediation Specifics of vSAN Clusters

Whether you manage a vSAN cluster with baselines or with a single image, remediating the hosts that are part of a vSAN cluster has its specifics.

When you remediate hosts that are part of a vSAN cluster, you must be aware of the following behavior:

- vSphere Lifecycle Manager puts only one host at a time in maintenance mode.
- vSphere Lifecycle Manager remediates hosts that are part of a vSAN cluster sequentially.
- Because vSphere Lifecycle Manager handles the remediation of the hosts sequentially, the host remediation process might take an extensive amount of time to finish.
- vSphere Lifecycle Manager remediates vSAN clusters with configured fault domains by upgrading all hosts from one fault domain first and then upgrading the hosts in the next fault domain.
- For a vSAN stretched cluster, vSphere Lifecycle Manager first remediates the hosts from the preferred site and then proceeds with remediating the hosts in the secondary site.

Host Maintenance Mode and vSAN Clusters

You can remediate a host that is in a vSAN cluster in two ways, depending on how you want to handle the virtual machines on the host:

- You can put the host in maintenance mode manually and remediate the host by using vSphere Lifecycle Manager.
- You can have the host enter maintenance mode during the vSphere Lifecycle Manager remediation process.

In the vSphere Client, when you put a host from a vSAN cluster into maintenance mode, you can choose between multiple options: Ensure accessibility, Full data evacuation, and No data evacuation. The Ensure accessibility option is the default option, and means that when you put a host in maintenance mode, vSAN ensures that all accessible virtual machines on the host remain accessible. To learn more about each of the options, see the "Place a Member of a vSAN Cluster in Maintenance Mode" topic in the *vSphere Storage* documentation.

During remediation, vSphere Lifecycle Manager, puts the hosts from the vSAN cluster in maintenance mode and handles the virtual machines on the host in the manner of the default Ensure accessibility option.

If a host is a part of a vSAN cluster, and any virtual machine on the host uses a VM storage policy with the setting for "Number of failures to tolerate=0", the host might experience unusual delays when it enters maintenance mode. The delay occurs because vSAN has to migrate the virtual machine data from one disk on the vSAN datastore cluster to another. Delays might take up to hours. You can work around this by setting the "Number of failures to tolerate=1" for the VM storage policy, which results in creating two copies of the virtual machine files on the vSAN datastore.

vSAN Health Check

vSphere Lifecycle Manager performs a remediation pre-check of vSAN clusters to ensure successful remediation. The vSAN health check is part of the remediation pre-check.

The vSAN health check gives you information about the cluster state and whether you must take extra actions to ensure successful remediation. Even if you do not take the recommended actions, you can still remediate the vSAN cluster or a host from the cluster. vSphere Lifecycle Manager successfully puts the host in maintenance mode and applies software updates on the host successfully. However, the host might fail to exit maintenance mode, and the remediation process might fail. As a result, the host from the vSAN cluster is upgraded, but you must take manual steps to take the host out of maintenance mode.

Using vSphere Lifecycle Manager Images to Remediate vSAN Stretched Clusters

When you manage a vSAN stretched cluster or a two-node ROBO cluster with vSphere Lifecycle Manager, you can manage the hosts in the cluster with a single image that is different from the image used to upgrade the dedicated witness host. With vSphere 8.0 Update 2, you upgrade the vSAN witness host in the same way as you upgrade a standalone host.

What Is a Stretched Cluster

A stretched cluster is a deployment model in which two or more hosts are part of the same logical cluster but are located in separate geographical locations. Every vSAN stretched cluster or two-node ROBO cluster has a witness host, which is a standalone host that is not a member of the respective cluster but is associated with it. The witness host of a vSAN cluster is managed by the same vCenter Server where the respective stretched or ROBO cluster resides.

vSphere Lifecycle Manager and the vSAN Witness Hosts

The vSAN witness host is a physical or virtual ESXi host that contains the witness components of virtual machine objects stored in the vSAN cluster. The witness host does not support workloads and is not a data node. A single stretched or two-node ROBO cluster can have only one witness host.

You can use vSphere Lifecycle Manager images to manage a vSAN stretched cluster and its witness host. Starting with vSphere 8.0 Update 2, you define separate images for the vSAN cluster and for the witness host. See Upgrading vSAN Stretched Clusters by Using a vSphere Lifecycle Manager Image. The following requirements exist:

- vCenter Server must be version 8.0 Update 2 and later.
- The witness host must be ESXi version 7.0 Update 2 and later.
- The witness host can be a virtual server or a physical server.
- The witness host can be a dedicated witness host or a shared witness host.
- The witness host must be upgraded before the hosts in the associated vSAN stretched or two-node cluster.
- The witness host and the associated vSAN clusters must not be upgraded in parallel.

- You cannot run virtual machines on a witness host. If vSphere Lifecycle Manager detects any stale virtual machines running on a witness host, during the remediation of the standalone host vSphere Lifecycle Manager sets the **VM power state** remediation setting to **Do not change power state**. For more information, see Configure vSphere Lifecycle Manager Remediation Settings for Clusters or Standalone Hosts that You Manage with a Single Image .

You start using vSphere Lifecycle Manager images to manage the witness host by performing any of the following tasks:

- You switch from using vSphere Lifecycle Manager baselines to using vSphere Lifecycle Manager images for an existing vSAN stretched or two-node ROBO cluster and for the dedicated standalone host.

  Note The transition to using images is blocked if the witness host is of ESXi version earlier than 7.0 Update 2. In such cases, you can use baselines to upgrade the witness host to version 7.0 Update 2 or later, and then you can start managing the witness host with a single vSphere Lifecycle Manager image.

- You convert an existing vSAN cluster that uses a single image into a stretched cluster with a virtual witness host.
- You upgrade to version 8.0 Update 2 and later for vCenter Server and version 7.0 Update 2 or later for the witness host.

You stop using vSphere Lifecycle Manager images to manage the witness host in the following cases:

- You convert an existing vSAN stretched cluster that uses images into a regular vSAN cluster.
- You deactivate vSAN for an existing vSAN stretched cluster that you manage with a single image.

Important With vSphere 8.0, you can use vSphere Lifecycle Manager images to manage standalone hosts in your vCenter Server inventory. Starting with vSphere 8.0 Update 2, you can apply a separate vSphere Lifecycle Manager image to the witness host of a vSAN cluster. You can start managing the witness host with a vSphere Lifecycle Manager image at the time of adding the host to the inventory or you can transition an existing standalone host that uses a single image to a witness host.

Upgrading vSAN Stretched Clusters by Using a vSphere Lifecycle Manager Image

You upgrade a stretched vSAN cluster along with the associated witness host by using a single vSphere Lifecycle Manager image, if the following requirements exist:

- vCenter Server must be version 7.0 Update 3 and later.
- The witness host must be ESXi version 7.0 Update 2 and later.
- The witness host is a virtual server and a dedicated witness host.

Starting with vSphere 8.0 Update 2, once you upgrade the vCenter Server instance to version 8.0 Update 2, the virtual dedicated witness host is no longer managed with the vSphere Lifecycle Manager image that you define for the vSAN cluster. You can use a full vSphere Lifecycle Manager image to upgrade a witness host in the same way you upgrade a standalone host. The desired image you apply on a witness host can contain a base ESXi image, and any user components, solution components, or OEM add-ons.

With vSphere 8.0 Update 2, for stretched vSAN clusters, you must first upgrade the witness host with the separate vSphere Lifecycle Manager image you configured and then proceeds to remediating the hosts in the preferred site and the secondary site. If all hosts in the preferred site are in a compliant state, then vSphere Lifecycle Manager skips the preferred site and starts remediating the hosts from the secondary site. If any host in the entire cluster is in an incompatible state, remediation stops. For more information about fault domain-aware remediation and the order in which vSphere Lifecycle Manager remediates the hosts in a vSAN cluster, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains .

To remediate the witness host against a single vSphere Lifecycle Manager image, the following requirements exist:

- vCenter Server must be version 8.0 Update 2 and later.
- The witness host must be ESXi version 7.0 Update 2 and later.
- The witness host can be a virtual server and a physical server.
- The witness host can be a dedicated witness host and a shared witness host.

Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains

In vSAN clusters with configured fault domains, vSphere Lifecycle Manager remediates the hosts in an order that vSphere Lifecycle Manager calculates by factoring in the defined fault domains.

What Is a Fault Domain?

A fault domain consists of one or more vSAN hosts grouped according to their physical location in the data center. When configured, fault domains enable vSAN to tolerate failures of entire physical racks as well as failures of a single host, capacity device, network link, or a network switch dedicated to a fault domain. You can configure fault domains for non-stretched and stretched vSAN clusters. For more information about configuring fault domains, see the *Administering VMware vSAN* documentation.

Upgrading vSAN Clusters Configured with Multiple Fault Domains

vSphere Lifecycle Manager remediates vSAN clusters with configured fault domains by remediating all hosts in one fault domain at a time. To define the order of fault domains, vSphere Lifecycle Manager calculates and assigns priority to each fault domain for the vSAN cluster.

Remediation starts with the fault domain that has the highest priority. The priority of a fault domain is determined by the number of non-compliant hosts in that fault domain. The fewer non-compliant hosts in a fault domain, the higher the priority of that fault domain. However, if multiple fault domains have the same priority, vSphere Lifecycle Manager selects the first fault domain from the list of fault domains.

After vSphere Lifecycle Manager selects a fault domain, vSphere Lifecycle Manager uses DRS recommendations to select the optimal host within that domain to be remediated.

For fault domain-aware remediation of vSAN clusters, the following requirements exist:

- vCenter Server must be version 7.0 Update 1 and later
- The ESXi hosts must be version 7.0 and later

Upgrading vSAN Clusters Enabled with NSX or vSphere IaaS control plane

You can remediate a vSAN cluster against a vSphere Lifecycle Manager image that contains the same ESXi version as the ESXi version currently on the hosts, but the latest versions of NSX and vSphere IaaS control plane components. In that case, vSphere Lifecycle Manager upgrades only those components, without upgrading the ESXi version. Even in those cases, vSphere Lifecycle Manager still recognizes the configured fault domains for the vSAN cluster and performs the solution upgrade in accordance with the fault domain configuration.

For fault domain-aware remediation of vSAN clusters with enabled NSX or vSphere IaaS control plane, the following requirements exist:

- vCenter Server must be version 7.0 Update 2
- The ESXi hosts version 7.0 and later

Updating Firmware in vSAN Clusters

You can use vSphere vSphere Lifecycle Manager images to upgrade the firmware of the servers that run in your vSAN clusters.

In a vSAN cluster, the SCSI controller firmware and the physical drive firmware are handling most of the data communication. To ensure your vSAN cluster health, you must perform controller firmware updates, when necessary.

Because firmware updates affect the hardware layer in your vSphere environment, they usually are rare events. Firmware updates occur during initial ESXi host setup or during major updates of vSphere or vSAN.

In earlier vSphere releases, firmware updates are delivered as baselines in the vSAN-managed baseline group. You must use a special vendor-provided tool that vSAN uses to detect, download, and install firmware updates. However, in vSphere 8.0, the recommendation baseline group that vSAN generates contains only patch updates and driver updates. It no longer contains firmware updates. As a result, you cannot use baselines to update the firmware in your vSAN clusters if the ESXi hosts are of version 7.0 and later. You can still use baselines to perform firmware updates on hosts of earlier versions, for example ESXi 6.7. But to perform firmware updates on hosts that are of ESXi version 8.0 and later and that are in a vSAN cluster, you

must manage that cluster with a single image. You must also deploy an OEM-provided hardware support manager and register it as a vCenter Server extension. The hardware support manager inspects the hardware of the hosts in the cluster and lists available and compatible firmware versions, which you can add to the image for the cluster. The actual firmware update happens upon remediating the cluster against an image that contains a firmware add-on.

For more information about the requirements for using images, see What Are the Requirements for Using vSphere Lifecycle Manager.

For more information about performing firmware updates by using images, see Firmware Updates with vSphere Lifecycle Manager.

About Recommendation Baseline Groups

vSAN creates system-managed baseline groups called recommendation baseline groups. You use recommendation baseline groups to upgrade the hosts in a vSAN cluster to the latest supported ESXi version, to patch the hosts with critical patches, or to update drivers on the host.

vSAN generates recommendation baseline groups automatically. If your vSphere environment does not contain any vSAN clusters, no recommendation baseline groups are generated. For each vSAN cluster in the vSphere inventory, vSphere Lifecycle Manager displays a single recommendation baseline group. You cannot edit or delete a recommendation baseline group and you cannot add it to custom baseline groups.

Recommendation baseline groups can contain any of the following sftware updates:

- An upgrade baseline that contains an ESXi upgrade image by a certified vendor with the latest tested and recommended version for the vSAN cluster.
- One or multiple patch baselines that contain recommended critical patches for the ESXi version of the hosts in the vSAN cluster.
- Recommended drivers for the ESXi hosts in the vSAN cluster.

Note Recommendation baseline groups no longer contain firmware updates. To update the firmware on your hosts, you must convert to using a single image for the vSAN cluster.

How Does vSphere Lifecycle Manager Generate Recommendation Baselines?

A vSAN recommendation engine regularly checks the current state of the software installed on the hosts in the vSAN cluster against the vSAN Hardware Compatibility List (HCL). If update recommendations are detected, the engine downloads all new critical patches and upgrade images and generates a vSAN cluster-level baseline. All available baselines are packed together in a recommendation baseline group and made available for use by vSphere Lifecycle Manager.

Every 24 hours, vSphere Lifecycle Manager runs an automatic check for a recommendation baseline group with build recommendations coming from vSAN. If a new recommendation baseline group is detected, vSphere Lifecycle Manager automatically attaches the vSAN recommendation baseline group to the vSAN cluster.

After refreshing the vSAN recommendation baseline group, vSphere Lifecycle Manager automatically performs a compliance check operation on the vSAN clusters against the updated recommendation baseline group. Operations such as adding and removing hosts from an existing vSAN cluster also trigger refresh of the attached recommendation baseline group, followed by a compliance check.

System Requirements for Using vSAN Recommendation Baseline Groups

- vCenter Server 7.0 or later.

  vSphere Lifecycle Manager runs as a service in vCenter Server 7.0 and later.
- vSAN cluster that contains hosts of ESXi version 6.0 Update 2 and later.
- Constant access of the vSphere Lifecycle Manager host machine to the Internet.

vSphere Lifecycle Manager and vSphere IaaS control plane

You can enable vSphere IaaS control plane on vSphere clusters that you manage with a single vSphere Lifecycle Manager image.

vSphere Lifecycle Manager and vSphere IaaS control plane with vSphere Networking

You start using vSphere IaaS control plane with vSphere networking on a cluster that uses a single vSphere Lifecycle Manager image by enabling the cluster for **Workload Management**. A cluster enabled for **Workload Management** is called a Supervisor. You enable a cluster for **Workload Management** from the **Workload Management** user interface in the vSphere Client.

Requirements

- Verify that all ESXi hosts in the Supervisor are version 7.0 Update 1 and later.
- Verify that the ESXi hosts in the Supervisor are assigned the required license.
- Verify that vCenter Server is version 7.0 Update 1 and later.
- **Note** You can manage the lifecycle of a Supervisor with either vSphere Lifecycle Manager baselines or vSphere Lifecycle Manager images. However, you cannot convert a Supervisor that uses vSphere Lifecycle Manager baselines to a Supervisor that uses vSphere Lifecycle Manager images. To use vSphere Lifecycle Manager images for a Supervisor, you must first switch the cluster which is not yet enabled for **Workload Management** to using images and then enable vSphere IaaS control plane on that cluster.
- Review the configuration requirements and additional information in *Working with vSphere Lifecycle Manager* chapter in the *Maintaining vSphere IaaS Control Plane* documentation.

Supported Workflows

The following workflows are supported for any Supervisor that uses vSphere Lifecycle Manager images and is configured to use the vSphere networking stack.

- You can upgrade a Supervisor to the latest version of vSphere IaaS control plane. You can also upgrade the ESXi version of the hosts in the Supervisor.

  You perform the upgrade of the Supervisor from the **Workload Management** user interface in the vSphere Client.

  You upgrade the ESXi version of the hosts in the Supervisor by remediating the cluster from the vSphere Lifecycle Manager user interface in the vSphere Client.

  Note You cannot perform a simultaneous upgrade of both vSphere IaaS control plane and ESXi.

- You deactivate vSphere IaaS control plane from the **Workload Management** user interface in the vSphere Client.You can deactivate vSphere IaaS control plane on a cluster that uses a single vSphere Lifecycle Manager image.

  When you deactivate vSphere IaaS control plane, you can use the cluster for traditional virtual machine workloads.

- You can add and remove hosts to and from a cluster that has both vSphere IaaS control plane and vSphere Lifecycle Manager enabled.

  For more information about adding and removing hosts to and from a cluster, see the *vCenter Server and Host Management* documentation.

For detailed information about working with a Supervisor that uses a single image, see the *Working with vSphere Lifecycle Manager* section in the *Maintaining vSphere IaaS Control Plane* documentation.

Upgrading the vSphere IaaS control plane Components in a vSAN Cluster

To upgrade the vSphere IaaS control plane components installed on the hosts in a cluster, you must remediate the cluster against a vSphere Lifecycle Manager image that contains the latest version of those vSphere IaaS control plane components.

In a vSAN cluster with configured fault domains, vSphere Lifecycle Manager recognizes the configured fault domains for the cluster and performs the solution upgrade in accordance with the fault domain configuration. If the vSAN cluster is a stretched cluster, you must upgrade the witness host separately, after vSphere Lifecycle Manager finishes remediating all fault domains. For more information about remediating vSAN stretched clusters and vSAN clusters configured with fault domains, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains . For more information about stretched clusters, see the *vSAN Planning and Deployment* documentation.

Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

vSphere Lifecycle Manager and vSphere IaaS control plane with NSX Networking

You can start using vSphere IaaS control plane with NSX networking on a cluster that uses a single vSphere Lifecycle Manager image by enabling the cluster for **Workload Management**. A cluster enabled with **Workload Management** is called a Supervisor. You enable the cluster for **Workload Management** from the **Workload Management** user interface in the vSphere Client. Upon enabling **Workload Management** on a Supervisor configured with the NSX networking stack, vSphere Lifecycle Manager installs the Spherelet VIB on every ESXi host in the cluster.

Requirements

- Verify that all ESXi hosts in the Supervisor are version 7.0 Update 2 or later.
- Verify that all ESXi hosts in the Supervisor are assigned the required license.
- Verify that vCenter Server is version 7.0 Update 2 or later.
- **Note** You can manage the lifecycle of a Supervisor with either vSphere Lifecycle Manager baselines or vSphere Lifecycle Manager images. However, you cannot convert a Supervisor that uses vSphere Lifecycle Manager baselines to a Supervisor that uses vSphere Lifecycle Manager images. To use vSphere Lifecycle Manager images for a Supervisor, you must first switch the cluster which is not yet enabled for **Workload Management** to using images and then enable vSphere IaaS control plane on that cluster.
- Review the configuration requirements and additional information in the *Working with vSphere Lifecycle Manager* chapter in the *Maintaining vSphere IaaS Control Plane* documentation.

Supported Workflows

The following workflows are supported for any Supervisor that uses vSphere Lifecycle Manager images and is configured to use the NSX networking stack.

- You can upgrade a Supervisor to the latest version of vSphere IaaS control plane. You can also upgrade the ESXi version of the hosts in the Supervisor.

  You perform the upgrade of the Supervisor from the **Workload Management** user interface in the vSphere Client. During upgrade, vSphere Lifecycle Manager upgrades the Spherelet VIB on the hosts to make it compatible with the new version of vSphere IaaS control plane or the new version of ESXi.

You upgrade the ESXi version of the hosts in the Supervisor by remediating the cluster from the vSphere Lifecycle Manager user interface in the vSphere Client.

Note You cannot perform a simultaneous upgrade of both vSphere IaaS control plane and ESXi.

- You deactivate vSphere IaaS control plane from the **Workload Management** user interface in the vSphere Client.You can deactivate vSphere IaaS control plane on a cluster that uses a single vSphere Lifecycle Manager image.

  When you deactivate vSphere IaaS control plane, you can use the cluster for traditional virtual machine workloads.

- You can add and remove hosts to and from a Supervisor that uses vSphere Lifecycle Manager images.

  When you add a host to a Supervisor that you manage with a single vSphere Lifecycle Manager image, vSphere Lifecycle Manager automatically installs the Spherelet VIB on the newly added host.

  When you remove a host from a Supervisor that you manage with a single vSphere Lifecycle Manager image, vSphere Lifecycle Manager removes the Spherelet VIB from the host. vSphere Lifecycle Manager also deletes the Spherelet VIB from a host that you move to another Supervisor.

  For more information about adding and removing hosts to and from a cluster, see the *vCenter Server and Host Management* documentation.

For detailed information about working with a Supervisor that uses a single image, see the *Working with vSphere Lifecycle Manager* chapter in the *Maintaining vSphere IaaS Control Plane* documentation.

Upgrading the vSphere IaaS control plane Components in a vSAN Cluster

To upgrade the vSphere IaaS control plane components installed on the hosts in a cluster, you must remediate the cluster against a vSphere Lifecycle Manager image that contains the latest version of those vSphere IaaS control plane components.

In a vSAN cluster with configured fault domains, vSphere Lifecycle Manager recognizes the configured fault domains for the cluster and performs the solution upgrade in accordance with the fault domain configuration. If the vSAN cluster is a stretched cluster, you must upgrade the witness host separately, after vSphere Lifecycle Manager finishes remediating all fault domains. For more information about remediating vSAN stretched clusters and vSAN clusters configured with fault domains, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains . For more information about stretched clusters, see the *vSAN Planning and Deployment* documentation.

Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

vSphere Lifecycle Manager and VMware NSX®

You can use vSphere Lifecycle Manager baselines for upgrade operations in environments with NSX 3.0. Starting with vSphere 7.0 Update 1 and NSX 3.1, you can also use vSphere Lifecycle Manager images to manage clusters that have NSX enabled.

Using vSphere Lifecycle Manager Baselines to Upgrade ESXi Hosts in an Environment With VMware NSX® 3.0

You can use vSphere Lifecycle Manager to upgrade the ESXi hosts in an environment where you have NSX enabled.

Requirements

- Verify that the ESXi hosts to upgrade are version 6.7 or later.
- vCenter Server version 6.7 or earlier
- NSX 3.0
- Verify that the vmknics on the ESXi host are properly configured and the DHCP server works properly.

Workflow

1 Upgrade vCenter Server to version 7.0.

   For more information about upgrading vCenter Server, see the *vSphere Upgrade* documentation.

2 Import an ESXi 7.0 ISO image to the vSphere Lifecycle Manager depot.

   For more information, see Import an ISO Image to the vSphere Lifecycle Manager Depot.

3 Download the NSX 3.0.0 NSX Kernel Module for VMware ESXi 7.0 from http://customerconnect.vmware.com.

4 Import the kernel module to the vSphere Lifecycle Manager depot.

   For more information, see Import Updates to the vSphere Lifecycle Manager Depot.

5 Create an upgrade baseline with the imported ESXi 7.0 ISO image.

   For more information, see Create, Edit, or Delete vSphere Lifecycle Manager Baselines and Baseline Groups .

6 Create an extension baseline with the uploaded NSX kernel module.

   For more information, see Create, Edit, or Delete vSphere Lifecycle Manager Baselines and Baseline Groups .

7 Create a baseline group that contains the newly created upgrade and extension baselines.

   For more information, see Create a Host Baseline Group.

8 Attach the baseline group to a cluster.

   For more information, see Attach Baselines and Baseline Groups to Objects.

9 Remediate the cluster against the attached baseline group.

   For more information, see Remediate ESXi Hosts Against a Single Baseline or Multiple Baselines.

Using vSphere Lifecycle Manager Images in an Environment With NSX 3.1

You can use NSX on a cluster that you manage with a single vSphere Lifecycle Manager image. As a result, you can use NSX Manager to install, upgrade, or remove NSX components on the ESXi hosts in a cluster that you manage with a single image.

Requirements

- Verify that all ESXi hosts in the cluster are version 7.0 Update 1 or later.
- Verify that vCenter Server is version 7.0 Update 1 or later.
- Verify that NSX is version 3.1 or later.
- Verify that a vSphere Distributed Switch (VDS) is configured to manage the NSX traffic.

Supported Workflows

The following workflows are supported for clusters that are enabled for both vSphere Lifecycle Manager images and NSX.

- You can enable NSX on a cluster that you manage with a single vSphere Lifecycle Manager image.

  You perform the operation by configuring a transport node profile (TNP) for the cluster in the NSX Manager. In the NSX Manager, you can either manually add a TNP to the cluster, or automatically generate one in the **Getting Started** wizard. You can continue leveraging individual transport node configurations, but you must always use a TNP for the clusters that you manage with a single vSphere Lifecycle Manager image. You cannot enable NSX on a cluster that uses a single vSphere Lifecycle Manager image if you choose to only use individual transport node configurations for the hosts in the cluster.

- You can add hosts to a cluster that you manage with a single vSphere Lifecycle Manager image and that is enabled with NSX. You can also remove hosts from such a cluster.

  You perform the add and remove host operations in the vSphere Client. When you add a host to the cluster, vSphere Lifecycle Manager automatically installs the NSX component to the newly added host. To add a host to a cluster that you manage with a single vSphere Lifecycle Manager image, the host must be added to the VDS associated with the TNP. Otherwise, the host cannot fully work with NSX.

When you move a host from one cluster that uses a single vSphere Lifecycle Manager image to another, vSphere Lifecycle Manager applies the target cluster's image together with the target NSX component to the newly added host. If a host is deleted from the vCenter Server inventory, the NSX component is uninstalled from the host.

For more information about adding and removing hosts to and from a cluster, see the *vCenter Server and Host Management* documentation.

- You can upgrade NSX 3.1 to a later version in a cluster that you manage with a single vSphere Lifecycle Manager image.

  You perform the operation from the NSX Manager.

- You can upgrade both NSX and ESXi in a single vSphere Lifecycle Manager remediation task. The workflow is supported only if you upgrade from NSX version 3.1.

  In the NSX Manager, you stage the NSX upgrade as part of the image that the cluster uses. From the vSphere Lifecycle Manager user interface in the vSphere Client, you can further edit the image and you initiate remediation of the cluster. During remediation, vSphere Lifecycle Manager applies both the NSX and ESXi upgrades to the hosts in the cluster. For more information, see the *Upgrading NSX Guide* documentation.

- You can switch from using vSphere Lifecycle Manager baselines to using a vSphere Lifecycle Manager image for a cluster that is enabled with NSX.
- You can uninstall NSX from a cluster that you manage with a single vSphere Lifecycle Manager image.
- You can check the compliance, generate a remediation pre-check report, and remediate a cluster that you manage with a single vSphere Lifecycle Manager image and that is enabled with NSX.

  You perform the check compliance, generate a remediation pre-check, and remediation operations in the vSphere Client. Whenever you change the NSX configuration in the NSX Manager, the compliance state of the cluster that you see on the **Updates** tab for the cluster in the vSphere Client changes to non-compliant. You can remediate non-compliant hosts and clusters in the vSphere Client or you can solve the issues that cause non-compliance in the NSX Manager.

- You can back up and restore NSX.
- You can export the vSphere Lifecycle Manager image of a cluster that is enabled with NSX and import this image to another cluster that has both vSphere Lifecycle Manager images and NSX enabled.

For detailed information about all workflows that you perform in the NSX Manager, see the *NSX Administration* documentation.

Upgrading the NSX Components in a vSAN Cluster

To upgrade the NSX components installed on the hosts in a cluster, you must remediate the cluster against a vSphere Lifecycle Manager image that contains the latest version of those NSX components.

In a vSAN cluster with configured fault domains, vSphere Lifecycle Manager recognizes the configured fault domains for the cluster and performs the solution upgrade in accordance with the fault domain configuration. If the vSAN cluster is a stretched cluster, you must upgrade the witness host separately, after vSphere Lifecycle Manager finishes remediating all fault domains. For more information about remediating vSAN stretched clusters and vSAN clusters configured with fault domains, see Using vSphere Lifecycle Manager Images to Remediate vSAN Clusters with Configured Fault Domains . For more information about stretched clusters, see the *vSAN Planning and Deployment* documentation.

Scalability

For information about the scalability that vSphere Lifecycle Manager supports, visit the VMware Configuration Maximums Matrix at https://configmax.vmware.com/.

Using vSphere Lifecycle Manager Images for Standalone Hosts with NSX 4.2 and later

You can use NSX on a standalone host that you manage with a vSphere Lifecycle Manager image. As a result, vSphere Lifecycle Manager becomes responsible for installing, upgrading, and removing NSX components on the host.

Requirements

- Verify that the standalone ESXi host and the vCenter Server instance are of version 8.0 Update 3 and later.
- Verify that NSX is of version 4.2 and later.

Supported Workflows

- You can enable NSX on a standalone host that uses vSphere Lifecycle Manager images.

  You perform the operation by configuring NSX on the individual host in the NSX Manager UI. For more information about how to configure individual hosts as transport nodes, see the *Prepare ESXi Individual Hosts as Transport Nodes* procedure in the *NSX Installation Guide*.
- You can uninstall NSX from a standalone host that you manage with a vSphere Lifecycle Manager image.
- You can switch from using vSphere Lifecycle Manager baselines to using vSphere Lifecycle Manager images for an existing standalone host that is prepared as a transport node.

During the eligibility check on the transport node, vSphere Lifecycle Manager performs several additional checks and allows the operation to continue in case all of the following conditions are met:

- The vCenter Server instance is of version 8.0 Update 3 and later.
- The ESXi host is of version 8.0 Update 3 and later.
- The NSX version on the standalone host is 4.2 and later.
- The **Multi NSX** mode is not enabled on the vCenter Server instance. See *Multiple NSX Managers Managing a Single VMware vCenter* in the *NSX Installation Guide*.

- You can upgrade both NSX and ESXi on the standalone host by using a single vSphere Lifecycle Manager remediation task. You run the remediation operation in the vSphere Client.
- You can add a standalone host that has NSX already installed to a data center or a folder and enable vSphere Lifecycle Manager on the host during this process.

  During the eligibility check on the host, vSphere Lifecycle Manager performs several additional checks and allows the operation to continue in case all of the following conditions are met:

  - The vCenter Server instance is of version 8.0 Update 3 and later.
  - The ESXi host is of version 8.0 Update 3 and later.
  - The NSX version on the standalone host is 4.2 and later.
  - The **Multi NSX** mode is not enabled on the vCenter Server instance. See *Multiple NSX Managers Managing a Single VMware vCenter* in the *NSX Installation Guide*.
- If you take a host out of a cluster that is prepared with a transport node profile (TNP) and is managed with a vSphere Lifecycle Manager image, the host becomes standalone. The host can retain the image of the cluster in case the following criteria are met:

  - The vCenter Server and ESXi host are of version vSphere 8.0 Update 3 and later.
  - NSX is of version 4.2 or later.
  - During the move operation the host stays connected or reachable.

  Otherwise, the image is removed from the host and the host is reverted back to using baselines.
- You can add a standalone host that used baselines to a cluster that you manage with a single vSphere Lifecycle Manager image and that is enabled with NSX.

  When you add the standalone host to the cluster, vSphere Lifecycle Manager automatically installs the NSX component to the newly added host. To add a host to a cluster that you manage with a single vSphere Lifecycle Manager image, the host must be added to the VDS associated with the TNP. Otherwise, the host cannot fully work with NSX.

Using vSphere Configuration Profiles to Manage Host Configuration at a Cluster Level

11

With vSphere Configuration Profiles, you can manage the configuration of all hosts in a cluster collectively. You set up a desired configuration that you can apply to all hosts in a single operation. You can also use a reference host and make its configuration the desired configuration for an entire cluster. Using vSphere Configuration Profiles ensures consistency in host configuration.

vSphere Configuration Profiles uses a declarative model to manage host configuration at a cluster level. With vSphere Configuration Profiles, you can perform the following tasks:

- Set a desired host configuration at a cluster level. The configuration is created and managed in the form of a human-readable JSON file backed by a JSON schema. Starting with vSphere 8.0 Update 2, you can edit the desired cluster configuration settings in the vSphere Client.
- Check the host compliance against the configuration for the cluster.
- Remediate the cluster to make non-compliant hosts compliant with the configuration set at the cluster level.

To perform all these tasks, you need the proper privileges. To view the full list of privileges required for using vSphere Configuration Profiles, see Required Privileges for Using vSphere Configuration Profiles

Starting with vSphere 8.0 Update 3, you can enable vSphere Configuration Profiles on a cluster that you manage with a single image and on a cluster that you manage with baselines. For clusters that you manage with baselines, you can also use vSphere Host Profiles, see the vSphere Host Profiles documentation.

You start using vSphere Configuration Profiles by enabling the feature during cluster creation or by transitioning to vSphere Configuration Profiles. You can switch from using host profiles to enabling and using vSphere Configuration Profiles at any time. The change is permanent. That is, if you switch to using vSphere Configuration Profiles, you cannot undo the transition.

For information about how to enable vSphere Configuration Profiles during cluster creation and set a desired configuration for the cluster, see Enable vSphere Configuration Profiles During Cluster Creation.

For information about how to switch from using legacy configuration management tools, such as host profiles, to using vSphere Configuration Profiles, see Transition to Using vSphere Configuration Profiles

System Requirements for Using vSphere Configuration Profiles

- Your vCenter Server instance and all ESXi hosts in a cluster managed with a single image must be of version 8.0 Update 1 and later.
- Your vCenter Server instance and all ESXi hosts in a cluster managed with baselines must be of version 8.0 Update 3 and later.
- Required privileges.

Limitations to Using vSphere Configuration Profiles

- You can't deactivate vSphere Configuration Profiles.
- With vSphere 8.0 Update 1, you can use vSphere Configuration Profiles if you use vSphere Distributed Switch for your cluster. Both, your vCenter Server instance and all ESXi hosts in the cluster managed with a single image, must be of version 8.0 Update 1.

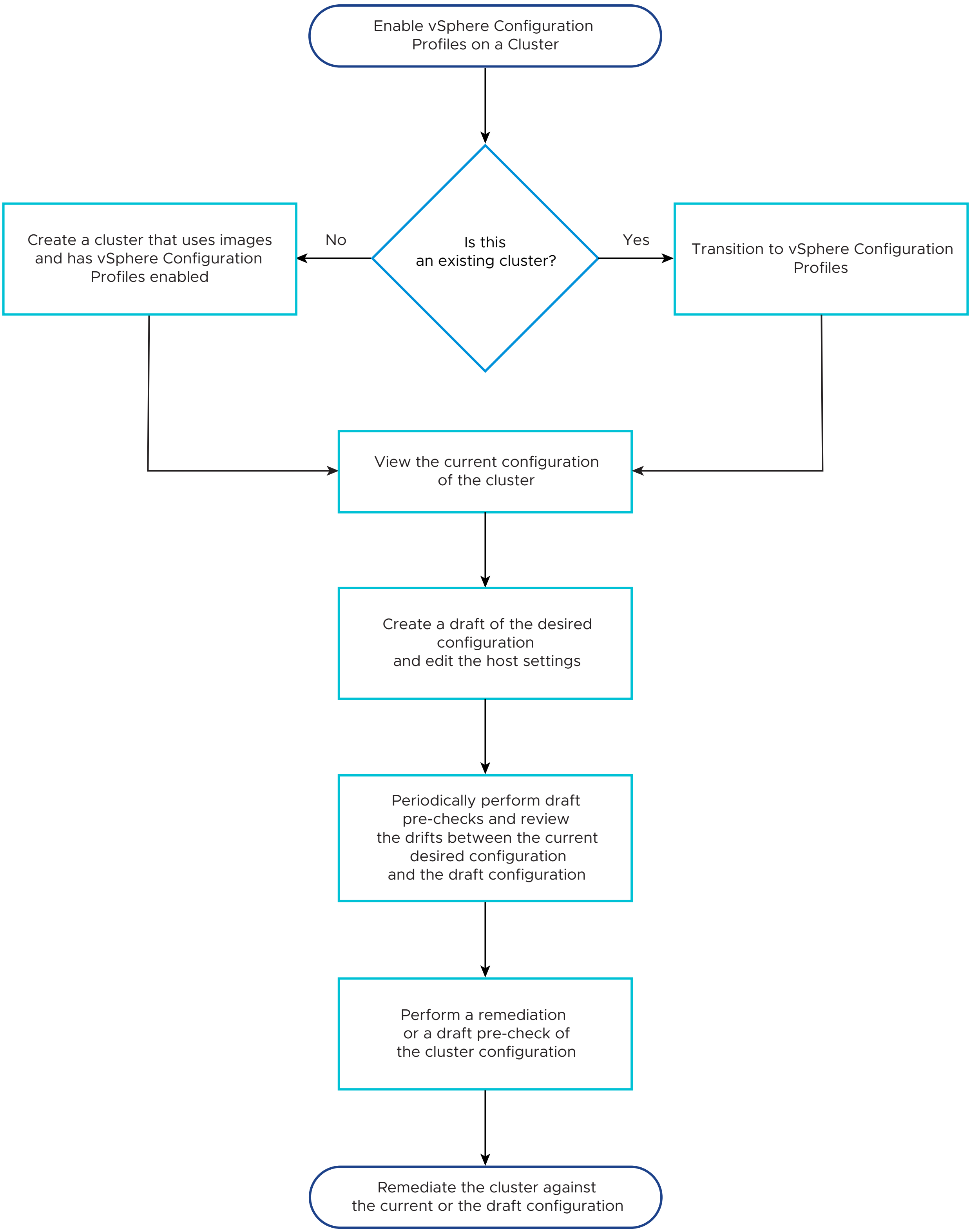
  Note Starting with vSphere 8.0 Update 3, you can manage the vSphere Distributed Switch configuration of the hosts in a cluster with enabled vSphere Configuration Profiles. You can also use the workflows for managing and configuring the vSphere Distributed Switches described in the *vSphere Networking* documentation.

- You can't enable vSphere Configuration Profiles on a cluster with DPU-backed hosts.
- You can't enable vSphere Configuration Profiles if NSX is also enabled for the cluster.

How to Start Using vSphere Configuration Profiles for Clusters That You Manage with a Single Image

You can enable vSphere Configuration Profiles during the cluster creation or you can transition an existing cluster managed with a vSphere Lifecycle Manager image to vSphere Configuration Profiles.

Figure 11-1. Enable vSphere Configuration Profiles on a Cluster That You Manage with a Single Image



When you enable vSphere Configuration Profiles during the cluster creation, the cluster is created with a default configuration and you must set up the desired cluster configuration by editing its settings. For more information, see Enable vSphere Configuration Profiles During Cluster Creation.

When you transition an existing cluster that you manage with a vSphere Lifecycle Manager image to vSphere Configuration Profiles, you set up a desired cluster configuration and as a result of the transitioning operation, all hosts in the cluster are compliant with the desired configuration. For more information, see Transition to Using vSphere Configuration Profiles.

Starting with vSphere 8.0 Update 2, you can create a draft configuration and edit the configuration settings directly in the vSphere Client. For more information, see Create a Draft Configuration in vSphere Client.

How to Start Using vSphere Configuration Profiles for Clusters That You Manage with Baselines

With vSphere 8.0 Update 3, you can enable vSphere Configuration Profiles during the cluster creation or you can transition an existing cluster managed with baselines to vSphere Configuration Profiles.

When you enable vSphere Configuration Profiles during the cluster creation operation, the cluster is created with an empty configuration. To create a desired cluster configuration, you must add at least one host to the cluster that you manage with baselines. Then you must select a reference host from which the configuration schema and the configuration settings are extracted and imported to the cluster as the desired cluster configuration. The reference host must be part of the cluster managed with baselines and must be of version 8.0 Update 3 and later. For more information, see Enable vSphere Configuration Profiles During Cluster Creation.

When you transition an existing cluster that you manage with baselines to vSphere Configuration Profiles, you use a host from the cluster as a reference host to set up the desired cluster configuration. When the transitioning operation completes, all hosts in the cluster are compliant with the desired configuration. For more information, see Transition to Using vSphere Configuration Profiles.

Read the following topics next:

- Enable vSphere Configuration Profiles During Cluster Creation
- Transition to Using vSphere Configuration Profiles
- Working with Configuration Documents and Configuration Schemas
- View Host Settings in the Desired Configuration
- Create a Draft Configuration in vSphere Client
- Edit the Host Settings of a Draft Configuration in vSphere Client
- Import a Configuration Document or a Configuration from a Reference Host Into an Existing Draft Configuration

- Delete a Draft Configuration for a Cluster
- Check Host Compliance Against the Desired Configuration for the Cluster
- Run a Remediation or a Draft Pre-Check
- Remediate a Cluster Against the Desired or Draft Configuration

Enable vSphere Configuration Profiles During Cluster Creation

You can enable vSphere Configuration Profiles during the process of creating a cluster. However, in this case, there are some steps which you must perform to create a desired cluster configuration.

If you create a cluster that you manage with a single image, it is created with a default configuration. You must define the desired configuration for the cluster by editing the default settings after the cluster is successfully created. In case you create a cluster that you manage with baselines, it is created with an empty configuration and you must add at least one host to the cluster before setting up the desired cluster configuration. To define the desired configuration for the cluster that you manage with baselines, you must use a reference host from the cluster.

The overall workflow for enabling vSphere Configuration Profiles on a cluster that you manage with a single image and setting up a desired configuration is the following:

1 Create a cluster. For more information, see Chapter 4 Creating and Managing vSphere Lifecycle Manager Clusters.

2 Set up the desired configuration for the cluster.

   Note Starting with vSphere 8.0 Update 2, you can use vSphere Client to create a draft configuration and edit the host configuration settings for a cluster in the user interface.

   - Option 1: Create a draft configuration by using one of the following options:
     - Reuse the settings of the default configuration for the cluster.
     - Reuse the configuration from an existing cluster by exporting its configuration document and importing it into the created draft configuration. See Import a Configuration Document or a Configuration from a Reference Host Into an Existing Draft Configuration
     - Reuse the configuration of one of the hosts in the cluster.

     After creating the draft configuration, edit the configuration settings to achieve the desired configuration for the cluster. For more information, see Create a Draft Configuration in vSphere Client and Edit the Host Settings of a Draft Configuration in vSphere Client.

- Option 2: Export the configuration schema for the newly created cluster and use it to create your own JSON configuration document, which you can import into the cluster.

  The exported configuration schema document follows the JSON Schema format. You use it to create and edit your own JSON configuration document in an external JSON editor tool.

- Option 3: Export the default or the draft configuration document of the cluster, edit the JSON file manually, and import it back into the cluster. You can also export and use the default or the draft configuration schema for the cluster to facilitate yourself in editing the desired configuration document.
- Option 4: Extract the settings from a host in the vCenter Server inventory and import them into the newly created cluster to use them as the common desired configuration.

The overall workflow for enabling vSphere Configuration Profiles on a cluster that you manage with baselines and setting up a desired configuration is the following:

1 Create a cluster and add at least one host to the cluster. For more information about creating a cluster, adding and removing hosts to and from a cluster, see the *vCenter Server and Host Management* documentation.

2 Set up the desired configuration for the cluster.

   - Option 1: Create a draft configuration by reusing the configuration of one of the hosts in the cluster as reference.

     After creating the draft configuration, edit the configuration settings to achieve the desired configuration for the cluster. For more information, see Create a Draft Configuration in vSphere Client and Edit the Host Settings of a Draft Configuration in vSphere Client.

   - Option 2: Export the configuration schema for the newly created cluster and use it to create your own JSON configuration document, which you can import into the cluster.

     The exported configuration schema document follows the JSON Schema format. You use it to create and edit your own JSON configuration document in an external JSON editor tool.

   - Option 3: Export the draft configuration document of the cluster, edit the JSON file manually, and import it back into the cluster. You can also export and use the default or the draft configuration schema for the cluster to facilitate yourself in editing the desired configuration document.

Transition to Using vSphere Configuration Profiles

For any cluster that you manage with a single image or with baselines, you can start using vSphere Configuration Profiles. The transition workflow allows you to enable vSphere Configuration Profiles on an existing cluster and set up the desired configuration for the cluster.

The transition workflow for a cluster that you manage with a single image starts with eligibility checks on the cluster and hosts. If the cluster is not eligible, the transition workflow cannot proceed. If the cluster is eligible, user can import a configuration from a host in the cluster or from a JSON file. The configuration is then validated. You can edit the configuration at this stage by using the export and import options. vSphere Configuration Profiles runs a pre-check to ensure that the configuration can be applied to all hosts. After you confirm the enablement of vSphere Configuration Profiles, eligibility checks are re-run and the cluster is remediated against the configuration that you set up.

Starting with vSphere 8.0 Update 3, you can enable vSphere Configuration Profiles on a cluster that you manage with baselines. The transition workflow starts with selecting a reference host which configuration schema is imported and used as a desired cluster configuration schema.

Starting with vSphere 8.0 Update 1, you can enable vSphere Configuration Profiles on a cluster that uses a vSphere Distributed Switch.

Note Staring with vSphere 8.0 Update 3, vSphere Configuration Profiles can manage the vSphere Distributed Switch configuration of the hosts in a cluster managed with a single image.

To manage any drifts related to the vSphere Distributed Switch configuration, you can use both options:

- The vSphere Distributed Switch workflows described in the *vSphere Networking* documentation
- The vSphere Configuration Profiles workflows described in this chapter.

Prerequisites

- Verify that vCenter Server and ESXi are of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image.
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that if the cluster uses vSphere Distributed Switch, vCenter Server and all ESXi hosts in the cluster are of version 8.0 Update 1 and later.
- Verify that if the cluster uses vSphere Distributed Switch and you want to manage the vSphere Distributed Switch configuration with vSphere Configuration Profiles, vCenter Server and ESXi are of version 8.0 Update 3 and later.
- Verify that the cluster is not empty.
- Verify that all hosts in the cluster are compliant with the image for the cluster if the cluster is managed with a single image.
- Verify that NSX is not enabled on the cluster.
- Verify that you have the required privileges for the transitioning operation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

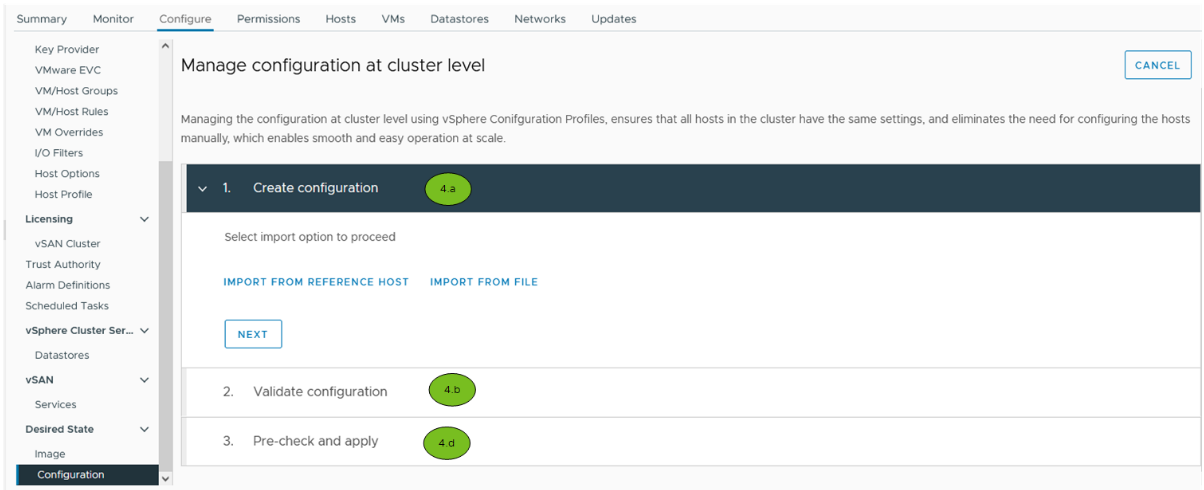
1 In the vSphere Client, navigate to a cluster that you manage with a single image or a cluster that you manage with baselines.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 Click **Create configuration**.

   The **Check Cluster Eligibility for Transition** task starts to ensure that the cluster is eligible for transitioning to vSphere Configuration Profiles.

4 In the **Manage configuration at cluster level** pane, follow the prompts to set up a desired configuration for the cluster and apply it to all hosts.



a Under **Create configuration**, select an import option and click **Next**.

- To import the configuration from a reference a host within the cluster, click **Import from reference host**, select the reference host, and confirm the import.

  Note This option is available for a cluster that you manage with baselines and for a cluster that you manage with a single image.

- To import the configuration from a JSON file that you created or edited, click **Import from file**, locate the JSON file with the configuration that you want to import and confirm the import.

  Note This option is only available for a cluster that you manage with a single image.

The **Validate Configuration for Transition** task starts to ensure that the imported configuration is valid and can be used as the desired configuration for the cluster.

b (Optional) Under **Validate configuration**, view the validation messages and edit the imported configuration.

- Click **Export configuration** to download the current configuration document and edit its settings.
- Click **Export configuration schema** to download the JSON file that represents the configuration schema.
- Click **Import configuration** to import the edited configuration document back into the cluster.

c Click **Next**.

The **Precheck Configuration for Transition** tasks starts to ensure that the configuration can be applied to all hosts successfully.

d Under **Pre-check and apply**, view pre-check details and remediation impact and click **Finish and apply**.

e In the **Finish and apply** dialog box, confirm that you want to apply the configuration to all hosts in the cluster.

vSphere Configuration Profiles is enabled for the cluster and the cluster is remediated against the configuration you set up during this operation.

f (Optional) Click **Go to configuration** to view and edit the cluster configuration settings.

You can cancel the transition at any stage of the workflow. Later, if you did not discard the changes that you made during the transition workflow, you can resume the transition and use the configuration imported before canceling the transition operation. If you want to start the whole process anew, discard all your changes. When you discard your changes, the imported configuration is also deleted.

Results

The cluster now uses vSphere Configuration Profiles to manage the configuration of its hosts. All hosts in the cluster are compliant with the desired configuration you set up during the transitioning operation.

What to do next

View the current desired cluster configuration. For more information, see View Host Settings in the Desired Configuration. You can also create a draft configuration and edit the host settings in the vSphere Client. For more information, see Create a Draft Configuration in vSphere Client.

Working with Configuration Documents and Configuration Schemas

You can manually edit the configuration settings for a cluster by using the configuration document and the configuration schema available for the current configuration and for the draft configuration of the cluster.

What Are the Configuration Schema and the Configuration Document

You set up and manage the desired host configuration for an entire cluster by working with the configuration document for the respective cluster. The configuration document is a JSON file that you can download to your local machine and edit with a JSON editor tool.

Starting with vSphere 8.0 Update 2, you no longer need to download the configuration document to edit it. Instead, you can directly edit the current cluster configuration in the vSphere Client. You create a working copy of the cluster configuration, called a draft, edit the configuration settings, and apply your changes to the cluster in a single operation. For more information, see Edit the Host Settings of a Draft Configuration in vSphere Client.

A valid configuration document contains a `profile` section and, optionally, a `host-specific` and `host-override` sections.

- The `profile` section contains common configuration that is applicable to all hosts in the cluster.
- The `host-specific` section represents configuration that can only be specified per host.
- The `host-override` section represents configuration that is overridden for a specific host in the cluster.

The configuration document is backed by a JSON schema, which is not editable. The configuration schema is a JSON file that represents the complete ESXi configuration. The schema follows the JSON Schema format and contains the default values for all host properties. The configuration schema is generated from the desired software specification defined in the image for the cluster. The configuration schema changes when you change the software specification for the cluster.

Export the Cluster Configuration or Cluster Configuration Schema

You can export the current cluster configuration in the form of a JSON file, which you can manually edit. You can also export the configuration schema for the cluster and use it to help you create your own configuration document from scratch or edit an exported configuration document.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 1 or later.
- Verify that ESXi is of version 8.0 Update 1 or later.
- Verify that you have the required license.
- Verify that you have the required privileges for the export operation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1. In the vSphere Client, navigate to a cluster that you manage with a single image.
2. On the **Configure** tab, click **Desired State > Configuration**.
3. On the **Settings** tab, select your task.
   - To download the current configuration for the cluster, from the **Export** drop-down menu, click **Cluster configuration**.
   - To download the configuration schema for the cluster, from the **Export** drop-down menu, click **Cluster configuration schema**.

   A dialog box appears that prompts you to download the JSON file that contains the current cluster configuration or the configuration schema.
4. Click **Download**.

Results

The current configuration document or the configuration schema is saved locally on your machine.

What to do next

Edit the configuration document or use the configuration schema to create a new JSON file with the desired host configuration for the cluster. Then, import the newly created or edited configuration document into the cluster.

Export the Draft Cluster Configuration or Draft Cluster Configuration Schema

You can export the draft cluster configuration in the form of a JSON file and manually edit it. You can also export the draft configuration schema for the cluster and use it to help you create your own configuration document from scratch or edit an exported configuration document.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 2 or later.
- Verify that ESXi is of version 8.0 Update 1 or later.
- Verify that you have the required license.
- Verify that you have a working copy of the configuration created for the cluster.
- Verify that you have the required privileges for the export operation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 On the **Draft** tab, select your task.

   - To download the current draft configuration document for the cluster, click the horizontal ellipses icon and select **Export**.
   - To download the draft configuration schema for the cluster, click the horizontal ellipses icon and select **Export configuration schema**.

   A dialog box appears that prompts you to download the JSON file that contains the current draft cluster configuration or the draft configuration schema.

4 Click **Download**.

Results

The current draft configuration document or the draft configuration schema is saved locally on your machine.

What to do next

Edit the draft configuration document or use the draft configuration schema to create a new JSON file with the desired host configuration for the cluster. Then, import the newly created or edited draft configuration document into the cluster.

Extract The Configuration from a Reference Host

You can extract the configuration of any host in the vCenter Server inventory. The configuration is saved on your local machine as a JSON file, which you can edit. You can import the extracted configuration into any other cluster that has vSphere Configuration Profiles enabled.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 1 or later.
- Verify that ESXi is of version 8.0 Update 1 or later.
- Verify that you have the required license.
- Verify that you have the required privileges for the extract operation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 On the **Settings** tab, click the **Export** drop-down menu and select **Reference host configuration**.

   The **Export Configuration** wizard opens.

4 Follow the prompts to download the configuration of the selected reference host.

   You can activate the **Show hosts from existing cluster** toggle to narrow down the list of hosts available in your vCenter Server to only the hosts available in the selected cluster.

Results

The configuration of a selected reference host is exported and downloaded to your local machine as a JSON file.

What to do next

Import the downloaded JSON configuration into another cluster to reuse the configuration. Alternatively, you can also edit the downloaded file first and then import it into the same or different cluster.

View Host Settings in the Desired Configuration

You can view information about how each host setting is configured in the current desired configuration for the cluster. For each host setting defined in the configuration document, you can see the values as defined for all hosts in the cluster and also any host overrides.

With vSphere 8.0 Update 2, the common settings, the host-specific settings, and the host overrides can be configured manually in the configuration document or in the vSphere Client. In the vSphere Client, you can view both, the settings of the currently applied desired configuration and the editable settings of the draft configuration of a cluster.

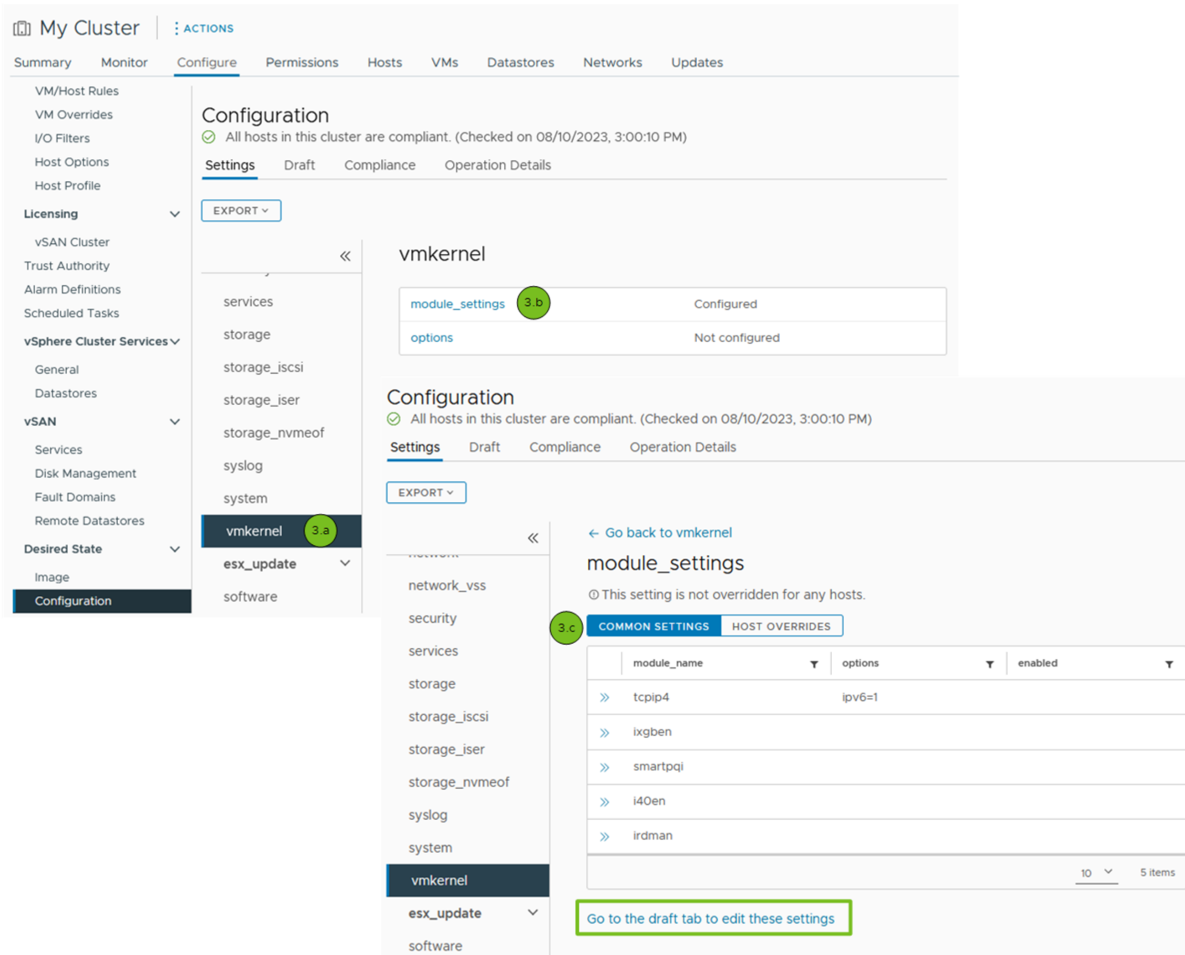
Prerequisites

- Verify that vCenter Server and ESXi are of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image.
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that you have the required license.
- Verify that you have the required privileges for viewing host settings in the desired configuration. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1. In the vSphere Client, navigate to a cluster that you manage with a single image or to a cluster that you manage with baselines.
2. On the **Configure** tab, click **Desired State > Configuration**.

3 On the **Settings** tab, view information about each setting defined in the current desired configuration document.



a Select a group of settings.

b In the panel on the right, select a setting that is configured.

c To view the common configuration for the selected setting, click **Common configuration**.

d To view host overrides for the selected setting, select **Host overrides** and select the host for which you want to see the overrides.

What to do next

Create a draft cluster configuration and edit the host settings by clicking on the **Go to the draft tab to edit these settings** link. For more information, see Create a Draft Configuration in vSphere Client.

Create a Draft Configuration in vSphere Client

When you want to make changes to the desired configuration of a cluster that uses vSphere Configuration Profiles, you can create a draft configuration for that cluster in the vSphere Client.

You can create only one draft configuration at a time for a cluster. When you finish making changes to the host settings, you must run a remediation pre-check before applying the changes to all host in the cluster and making your draft configuration the new desired cluster configuration.

Note More than one user with the required privileges can create a draft configuration for a cluster at the same time. When one of the users remediates the cluster with their draft configuration making it the desired configuration for the cluster, the other users editing their draft configurations for the same cluster will see an error message.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 2 or later and ESXi is of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image.
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that you have the required license.
- Verify that you are using vSphere Configuration Profiles for the cluster.
- Verify that you have the required privileges for the operation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image or to a cluster that you manage with baselines.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 On the **Draft** tab, choose the method of creating a draft configuration for the cluster.

Option	Steps
Create a copy of the current cluster configuration	To create a working copy from the current cluster configuration, click **Create draft**. ■ If you enabled vSphere Configuration Profiles during cluster creation, the draft configuration contains the default settings of the cluster that you manage with a single image retrieved from the desired cluster image. ■ If you transition a cluster that you manage with a single image or a cluster that you manage with baselines to using vSphere Configuration Profiles, the draft configuration is created from the desired cluster configuration.
Import a configuration document into a cluster and edit it as a draft configuration	This option for creating a draft configuration is available only for clusters that you manage with a single image. a On the **Draft** tab, select **Import from file**. The **Import Configuration from File** dialog box appears. b Click **Browse** to locate the file that you want to import and click **Import**. c Click **Close**.
Import the configuration from one of the hosts in the cluster	Use this option to import the configuration from one of the hosts in the cluster managed with a single image or with baselines. **Tip** If you enabled vSphere Configuration Profiles during cluster creation and the cluster is managed with baselines, a default draft configuration is not available for the cluster and you must use this option to import one from a reference host in the cluster a On the **Draft** tab, select **Import from host**. The **Select reference host** dialog box appears. b Select one of the hosts listed for the cluster and click **Import**. **Note** During the import operation, the configuration of the reference host is extracted and is compared to the current configurations of all hosts in the cluster. If a host in the cluster has configuration settings that differ from the settings of the reference host, these settings are marked in the draft configuration as host overrides. You can view the host overrides for a specific host setting on the **Host overrides** tab for that setting or under the `host-override` section of the draft configuration document.

Results

You created a draft configuration of the cluster which you can use to edit the host settings in the vSphere Client.

What to do next

You can edit the host settings within the draft configuration and remediate the cluster against the draft configuration in a single operation. For more information, see Edit the Host Settings of a Draft Configuration in vSphere Client.

Edit the Host Settings of a Draft Configuration in vSphere Client

You can create a draft configuration for a cluster and edit the host settings in the vSphere Client.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 2 or later and ESXi is of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image.
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that you have the required license.
- Verify that you have a draft configuration created for the cluster.
- Verify that you have the required privileges for performing remediation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image or to a cluster that you manage with baselines.

2 On the **Configure** tab, click **Desired State > Configuration**.

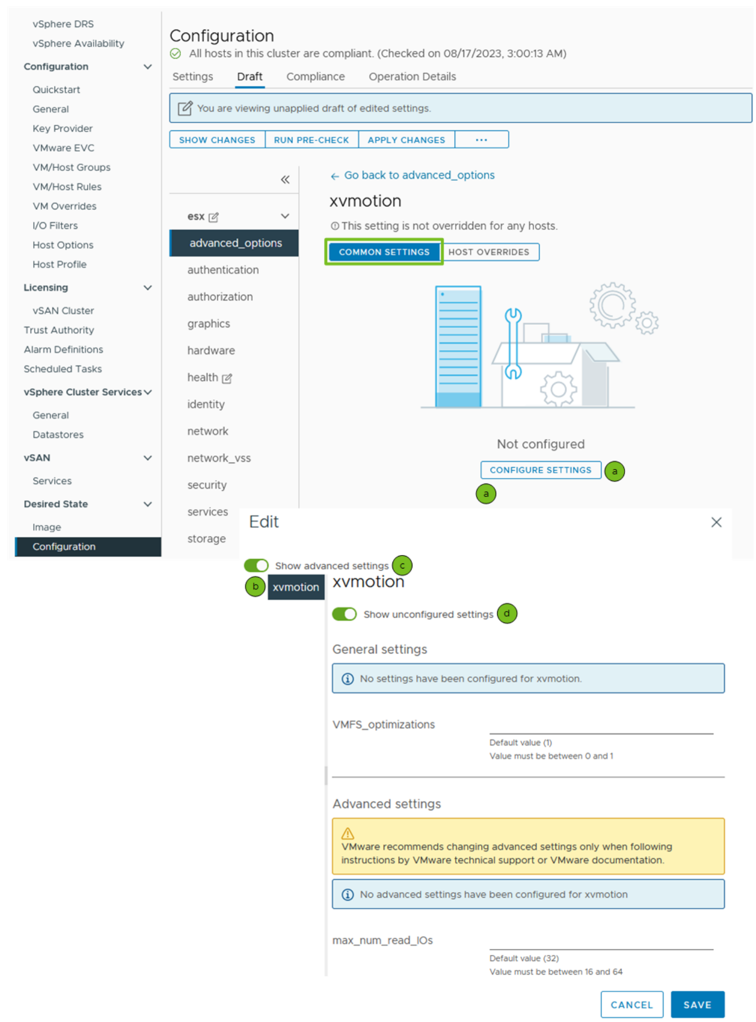
3 On the **Draft** tab, navigate to the host setting that you want to edit.

4 Edit the host setting of the draft configuration.

<table>
<tr><th>Option</th><th>Steps</th></tr>
<tr><td>Configure a common setting that has no existing configuration</td><td>
a On the Common settings tab, click Configure settings.

The Edit dialog box appears.

Figure 11-2. Configure a common setting



b Select the common setting from the left sidebar and configure its value.

The settings of the selected item appear on the right of the Edit dialog box.

c (Optional) Activate the Show advanced settings toggle, to view and edit the advanced settings.

If there is at least one advanced setting configured, the Show advanced settings toggle is automatically activated.

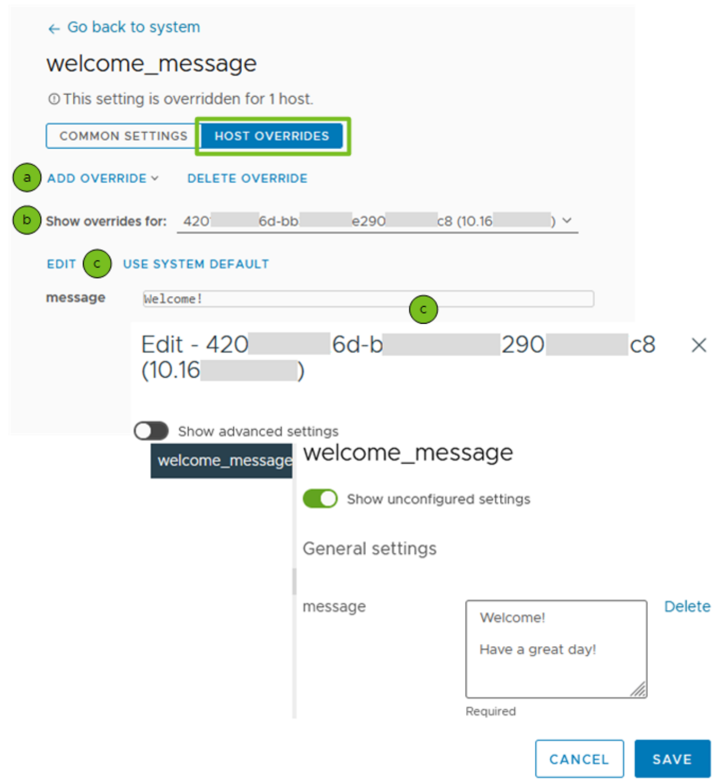
d (Optional) Deactivate the Show unconfigured settings toggle, to view and edit only the configured settings. By default, the toggle is activated.

e Click Save.

The configured settings appear under the Common settings tab.
</td></tr>
<tr><td>Edit a common setting that is</td><td>a On the Common settings tab, navigate to the current configuration for</td></tr>
</table>

Option	Steps
already configured	the selected setting and select it from the tree on the left. b Click **Edit**. The **Edit** dialog box appears. c Navigate to the configured setting by clicking on the **View settings** links and edit the value of the setting. d Click **Save**.

<table>
<tr><th>Option</th><th>Steps</th></tr>
<tr><td>Delete a common setting configuration</td><td>a On the Common settings tab, select the setting you want to delete from the list of configured settings and click Delete.
b Click Delete setting to confirm the deletion of the setting configuration.</td></tr>
<tr><td>Add a host override for a configured common setting</td><td>a On the Host overrides tab, click the Add override drop-down menu and select an option.
To add a host override by filtering the available hosts in the cluster using their host names, click Add override by host name.
The Add override for <setting_name> dialog box appears.
Select a host and click Add override.
To add a host override by filtering the hosts using their BIOS UUID, click Add override by BIOS UUID.
The Add override for <setting_name> dialog box appears.
Enter the BIOS UUID of the host in the respective field and click Add override.
You can use this option to add a host override for a host that is not currently part of the cluster.
b From the Show overrides for drop-down menu, select the host override that you created.
The configured common setting with its value appear under the drop-down menu.
c Select from the options for editing.
To edit the current configuration of the common setting, click Edit.
The Edit - <BIOS UUID (<host_name>)> dialog box appears.</td></tr>
</table>

Option	Steps
	Figure 11-3. Edit a host override for a configured common setting  Navigate to the configured setting and change its value. ■ To apply the system default configuration which can be different from the common configuration of the setting, click **Use system default** and confirm your choice.

Results

The settings of the draft configuration are configured.

What to do next

You can view the changes between the current draft configuration and the desired configuration of the cluster by clicking **Show changes** on the **Draft** tab. You can run a draft pre-check to validate the draft configuration and ensure that it can be applied on all hosts in the cluster. For more information, see Run a Remediation or a Draft Pre-Check. You can also remediate the cluster against the draft configuration and make it the new desired cluster configuration. For more information, see Remediate a Cluster Against the Desired or Draft Configuration.

Import a Configuration Document or a Configuration from a Reference Host Into an Existing Draft Configuration

For any cluster that uses vSphere Configuration Profiles and has a draft configuration created, you can override and replace the configuration settings by importing a valid configuration document or using the configuration settings of a reference host in the cluster.

You can import the configuration document of another cluster and reuse the configuration defined in that other cluster. You can also import a configuration document that you manually edited or created from scratch. You can also import the settings of one of the hosts available in the cluster and use them as common settings for all hosts in the cluster.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 2 or later and ESXi is of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image.
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that you have the required license.
- Verify that you have a draft configuration created for the cluster.
- Verify that you have the required privileges for the import operation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image or to a cluster that you manage with baselines.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 On the **Draft** tab, select your task.

Import Option	Steps
Import a JSON file	a To import a configuration document, click the horizontal ellipses and select **Import from file**. The **Import Configuration from File** dialog box appears. b Click **Browse** to locate the file that you want to import and click **Import and overwrite draft**.
Import the configuration of a reference host in the cluster	a To import the configuration settings from a reference host in the cluster, click the ellipses and select **Import from host**. The **Select reference host** dialog box appears. b Click the radio button for the respective host which configuration settings you want to use and click **Import and overwrite draft**.

4 Click **Close**.

Results

The imported configuration settings become the new draft configuration for the entire cluster.

When you replace the settings in the draft configuration with the settings of a single host from the cluster, these settings become the common settings for all hosts in the cluster. If a host in the cluster has settings that differ from the new common settings for the cluster, the original host settings are saved in the new draft configuration as host overrides.

What to do next

You can view the changes applied to the edited draft configuration of the cluster by clicking on **Show changes**. You can also starts a draft pre-check to ensure that the configuration is valid and to compute the remediation impact on all hosts in the cluster. Then you can remediate the cluster to make all non-compliant hosts compliant.

Delete a Draft Configuration for a Cluster

You can discard all changes that you made to a draft configuration by deleting it in the vSphere Client. The current desired state of the cluster remains unaffected.

When you create and edit a draft configuration, your changes are stored on vCenter Server. When you delete your draft configuration, the changes you made will be permanently lost. If another user creates a draft configuration for the same cluster, that draft configuration remains unaffected when you delete your draft configuration. You can preserve your current cluster configuration and continue editing the draft configuration settings only if you export the draft configuration document. For more information, see Export the Draft Cluster Configuration or Draft Cluster Configuration Schema.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 2 or later.
- Verify that ESXi is of version 8.0 Update 1 or later.
- Verify that you have a draft configuration created for a cluster.
- Verify that you have the required license.
- Verify that you have the required privileges for viewing host settings in the desired configuration. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 On the **Draft** tab, click the horizontal ellipses icon and select **Discard draft**.

   The **Discard draft** dialog box appears.

4 Click **Discard draft**.

Results

The draft configuration is permanently removed and you can no longer edit its settings.

What to do next

Create a new draft configuration if you want to edit the cluster configuration in the vSphere Client. For more information, see Create a Draft Configuration in vSphere Client.

Check Host Compliance Against the Desired Configuration for the Cluster

You can check the compliance of each host in a cluster only against the desired configuration set for the entire cluster. If a host is out of compliance with the desired configuration, you can see detailed information about the settings that make the host non-compliant.

The **Check Cluster Configuration Compliance** task runs automatically when you add a host to the cluster. You can manually run a compliance check only on the current desired configuration of the cluster.

Starting with vSphere 8.0 Update 1, you can enable vSphere Configuration Profiles on a cluster that contains hosts connected to a vSphere Distributed Switch. If you add a host connected to a vSphere Standard Switch to a cluster that contains hosts connected to a vSphere Distributed Switch, vSphere Configuration Profiles shows the added host as non-compliant. You must use the vSphere Distributed Switch workflows to remediate the host and make the host compliant with the desired cluster configuration. For more information about how to add a host to a vSphere Distributed Switch, see the *vSphere Networking* documentation.

Note In vSphere 8.0 Update 3, vSphere Configuration Profiles can manage the vSphere Distributed Switch configuration of the hosts in a cluster managed with a desired configuration. You can also use the workflows for managing and configuring the vSphere Distributed Switches described in the *vSphere Networking* documentation.

Prerequisites

- Verify that vCenter Server and ESXi are of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image.
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that you have the required license.
- Verify that you have the required privileges for checking compliance. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image or to a cluster that you manage with baselines.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 On the **Compliance** tab, click **Check compliance**.

   The **Check Cluster Configuration Compliance** task starts. After the task finishes, a list of all non-compliant hosts shows on the **Compliance** tab.

4 View the compliance results for each non-compliant host in the cluster.

   a On the **Compliance** tab, select a host from the **Hosts** list.

      An information panel appears on the right. You see the host settings and the respective desired and current values that cause the noncompliance.

What to do next

Remediate the cluster to make all non-compliant hosts compliant.

Run a Remediation or a Draft Pre-Check

You run a remediation pre-check to ensure that the desired configuration is valid and compatible with the current state of the hosts in the cluster, and that the cluster is in good health. You run a draft pre-check to ensure that the draft configuration is valid and can be applied on all hosts in the cluster. A pre-check that finds no issues means that you can successfully remediate the cluster and apply the desired or draft configuration to all hosts.

With vSphere 8.0 Update 2, you can create a draft of the cluster configuration in the vSphere Client and edit the configuration settings directly in the user interface. Before applying the draft configuration on a cluster, you can run a draft pre-check.

During a remediation or a draft pre-check, vSphere Configuration Profiles runs various checks on each host and the entire cluster to estimate and validate the impact of the desired or the draft configuration on the current state of the hosts in the cluster. The remediation and draft pre-checks also compute the remediation impact on the hosts.

With vSphere 8.0 Update 1, you can enable vSphere Configuration Profiles on a cluster that has hosts connected to a vSphere Distributed Switch. If you add a host that is connected to a vSphere Standard Switch to such cluster, the remediation pre-check returns an error and you cannot remediate the cluster before you manually add this host to the vSphere Distributed Switch. For more information about how to add a host to a vSphere Distributed Switch, see the *vSphere Networking* documentation.

Note In vSphere 8.0 Update 3, vSphere Configuration Profiles can manage the vSphere Distributed Switch configuration of the hosts in a cluster managed with a desired configuration. You can also use the workflows for managing and configuring the vSphere Distributed Switches described in the *vSphere Networking* documentation.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 1 or later, if you want to run a remediation pre-check of the desired configuration on a cluster that you manage with a single image.

- Verify that vCenter Server is of version 8.0 Update 2 or later, if you want to run a draft pre-check on a cluster that you manage with a single image..
- Verify that you have a draft configuration created, if you want to run a draft pre-check.
- Verify that ESXi is of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that you have the required license.
- Verify that you have the required privileges for running a remediation or a draft pre-check task. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1. In the vSphere Client, navigate to a cluster that you manage with a single image or to a cluster that you manage with baselines.
2. On the **Configure** tab, click **Desired State > Configuration**.
3. Start a pre-check by selecting one of the following options.
   - To run a remediation pre-check of the current desired configuration, on the **Compliance** tab, click **Run pre-check**.

     The **Cluster Configuration Remediation Pre-Check** task starts.
   - To run a draft pre-check of the edited cluster configuration, on the **Draft** tab, click **Run pre-check**.

     The **Cluster Configuration Draft Pre-check** task starts.
4. (Optional) Click the **Operation Details** tab to view details about the remediation or draft pre-check operations.

   The **Operation Details** tab gives summarized information or detailed information about the remediation operation, the remediation pre-check, or the draft pre-check operations. Any issues during those operations are also listed on the **Operation Details** tab.

What to do next

Fix all issues that are reported during the remediation or the draft pre-check and remediate the cluster.

Remediate a Cluster Against the Desired or Draft Configuration

You remediate a cluster against the desired or draft configuration to make all non-compliant hosts compliant with the configuration for the cluster.

Starting with vSphere 8.0 Update 2, you can create a draft of the cluster configuration in the vSphere Client and edit the configuration settings directly in the user interface. To make all hosts in the cluster compliant with the draft configuration, you must apply it to the cluster. The apply operation first sets the draft configuration as the new desired configuration for the cluster and then remediates all hosts in the cluster against the new desired configuration.

Before the cluster is remediated, an automatic remediation or draft pre-check is triggered. As a result, the remediation impact is calculated for each host in the cluster. The remediation might require a reboot or the host to enter maintenance mode.

Starting with vSphere 8.0 Update 1, you can enable vSphere Configuration Profiles on a cluster that contains hosts connected to a vSphere Distributed Switch. You can't use vSphere Configuration Profiles to manage the vSphere Distributed Switch configuration of the hosts in the cluster. You must manually fix any drifts in the vSphere Distributed Switch networking configuration of each non-compliant host in the cluster before you start the remediation task.

Note In vSphere 8.0 Update 3, vSphere Configuration Profiles can manage the vSphere Distributed Switch configuration of the hosts in a cluster managed with a desired configuration. You can also use the workflows for managing and configuring the vSphere Distributed Switches described in the *vSphere Networking* documentation.

Prerequisites

- Verify that vCenter Server is of version 8.0 Update 1 or later, if you want to remediate a cluster managed with a single image against the desired configuration.
- Verify that vCenter Server is of version 8.0 Update 2 or later, if you want to remediate a cluster managed with a single image against a draft configuration.
- Verify that ESXi is of version 8.0 Update 1 or later for using vSphere Configuration Profiles on a cluster that you manage with a single image.
- Verify that vCenter Server and ESXi are of version 8.0 Update 3 or later for using vSphere Configuration Profiles on a cluster that you manage with baselines.
- Verify that you have the required license.
- Verify that at least one of the hosts in the cluster is out of compliance with the desired configuration.
- Verify that you have the required privileges for performing remediation. See Required Privileges for Using vSphere Configuration Profiles.

Procedure

1 In the vSphere Client, navigate to a cluster that you manage with a single image or to a cluster that you manage with baselines.

2 On the **Configure** tab, click **Desired State > Configuration**.

3 Start the remediation operation.

- To remediate the cluster against the current desired configuration, on the **Compliance** tab, click **Remediate**.
- To remediate the cluster against the draft configuration, on the **Draft** tab, click **Apply changes**.

The **Remediate** wizard opens. A remediation pre-check task starts automatically to ensure that remediation can run without issues.

4 On the **Pre-check** page, wait for the remediation pre-check to finish, view the pre-check results and click **Next**.

5 On the **Review Impact** page, review the summary of the remediation impact on the cluster and on each host individually.

6 Click **Remediate** to close the **Remediate** wizard.

The **Remediate Cluster Configuration** task starts.

7 (Optional) Click the **Operation Details** tab to view details about the remediation, the remediation pre-check, or the draft pre-check operations.

The **Operation Details** tab gives summarized information or detailed information about the remediation operation or the remediation and draft pre-check operations. Any issues during those operations are listed on the **Operation Details** tab.

Results

All hosts in the cluster are compliant with the desired configuration.

Note More than one user with the required privileges can create a draft configuration for a cluster at the same time. If one of the users remediates the cluster with their draft configuration, the draft configuration becomes the new desired configuration for the cluster. In case another user attempts to remediate the cluster with their draft configuration at the same time, the remediation operation fails with an error. That user can either discard his draft configuration and start anew, or export their current draft and import it at a later time.

Backup and Restore Scenarios When Using vSphere Lifecycle Manager

12

Restoring a vCenter Server instance from a backup might impact the clusters in your environment in a seemingly unexpected way. Whether you use images or baselines to manage your clusters, vSphere Lifecycle Manager behaves in a specific manner during backup and restore operations.

When you back up a vCenter Server instance, you create a backup copy of all clusters in that vCenter Server instance.

Restoring vCenter Server After Switching from Baselines to Images for Cluster Lifecycle Management

Cluster A is a cluster that you manage by using baselines. You back up the vCenter Server instance where the cluster is. After the backup, you switch from using baselines to using images to manage cluster A and you remediate the cluster to apply the image to the hosts in the cluster. You now manage the lifecycle of cluster A by using a single cluster image.

If for some reason you must restore the vCenter Server instance from the backup copy you created, the restored vCenter Server instance contains cluster A. Because cluster A was managed through baselines at the time when you backed up the vCenter Server system, the restored vCenter Server instance contains cluster A, but you must again use baselines to manage it.

Restoring vCenter Server After Remediating a Cluster Managed by an Image

After remediation, cluster A uses image X with components Y to manage all hosts in the cluster collectively. At a point in time T, you back up the vCenter Server system. Later, you remediate the cluster against a new image X+1 with new components Y+1. Now all hosts in the cluster use image X+1 with components Y+1.

If for some reason you must restore the vCenter Server system from the backup copy that you created at time T, the restored vCenter Server instance contains cluster A, but the compliance check lists the hosts in the cluster as incompatible with the image that cluster A uses. The reason for the incompatibility is that after the restore operation, cluster A reverts back to using image X with components Y, while the hosts in the cluster still run image X+1 with components Y+1. Because you cannot downgrade ESXi, to make the hosts compliant with the cluster image, you must upgrade the cluster to image X+1 with components Y+1.